Liceo Classico Linguistico e Scienze Umane B.R. Motzo

Sede: Via Don Sturzo, 4, 09045 Quartu Sant'Elena (CA)
Telefono: 070/825629 **Sito istituzionale:** liceomotzo.edu.it
E-mail: CAPC09000E@istruzione.it **PEC:** CAPC09000E@pec.istruzione.it
C.U.: UFAGLG **C.F.:** 92168540927

REGOLAMENTO PROTEZIONE DATI

Glossario

Ai fini del presente regolamento si adottano le seguenti definizioni:
RGDP: Regolamento Generale sulla Protezione dei Dati Personali, Regolamento UE n. 679/2016;
Codice Privacy (di seguito anche Codice): D.lgs. 196/2003 e s.m.i.;
RPD: Responsabile della Protezione dei dati (in inglese **DPO** Data Protection Officer);
RPC: Responsabile della Prevenzione della Corruzione e della Trasparenza;
DPIA: Valutazione di impatto sulla protezione dei dati;
Privacy by design: Privacy dal momento della sua progettazione. Implica che qualsiasi progetto va realizzato assumendo dalla fase iniziale di ideazione misure di protezione di dati personali;
Privacy by default: protezione dei dati per impostazione predefinita, ovvero, misure tecniche ed organizzative che assicurano solo i dati personali necessari per ogni specifica finalità di trattamento;
Audit Privacy: è una valutazione dei processi interni adottati sul grado di rispetto della normativa vigente del Reg. UE n. 679/2016;
GEPD: Garante Europeo della protezione dei dati;
Accountability: letteralmente "rendere conto", ovvero, il Titolare del trattamento deve rendere conto delle azioni intraprese per garantire che i trattamenti dei dati effettuati all'interno dell'amministrazione siano conformi ai principi stabiliti nell'RGDP e nella normativa nazionale di riferimento.
EDPB: European Data Protection Board Organismo consultivo ed indipendente che ha il compito di assicurare la corretta applicazione della normativa privacy e di fornire consulenza, approfondimenti e pareri in merito al RGPD. Dall'entrata in vigore del RGPD recepisce, tra le altre, le funzioni del gruppo di lavoro ex Art. 29 (**WP29**).
Dati personali: Qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;
Trattamento: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;
Limitazione di trattamento: il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro;
Profilazione: qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica;
Archivio: qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico;
Pseudonimizzazione: il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile;

Titolare del trattamento: La persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;
Responsabile del trattamento: persona fisica o giuridica o ente pubblico che tratta i dati per conto del Titolare del trattamento;
Destinatario: la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerate destinatari; il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento;
Terzo: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile;
Consenso dell'interessato: qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento;
Violazione dei dati personali (Data breach): la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati;
Dati relativi alla salute: i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute;
Dati giudiziari: i dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza.
Autorità di controllo: l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51 RGPD;

TITOLO I
PRINCIPI

Art. 1
Finalità e quadro normativo di riferimento

1. Il presente regolamento disciplina le misure organizzative ed i processi interni di attuazione del Regolamento UE n. 679/2016 (RGPD) ai fini del trattamento di dati personali per finalità istituzionali nel Liceo Classico Linguistico e Scienze Umane B.R. Motzo.
2. Ai fini del presente regolamento, per funzioni istituzionali si intendono quelle:
   a) previste dalla legge, dal Piano Triennale dell'Offerta Formativa (PTOF), dai regolamenti e da atti amministrativi generali;
   b) esercitate in attuazione di convenzioni, accordi nonché sulla base degli strumenti di programmazione e pianificazione previsti dalla legislazione vigente;
   c) svolte per l'esercizio dell'autonomia organizzativa, amministrativa e finanziaria dell'istituto;
   d) in esecuzione di un contratto con i soggetti interessati, qualora stipulato in relazione alle proprie finalità e compiti istituzionali.
3. Il titolare garantisce che il trattamento dei dati, a tutela delle persone fisiche, si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali, a prescindere dalla loro nazionalità o dalla loro residenza. Il titolare, nell'ambito delle sue funzioni, gestisce gli archivi e le banche dati rispettando i diritti, le libertà fondamentali e la dignità delle persone, con particolare riferimento alla riservatezza e all'identità personale. Ai fini della tutela dei diritti e delle libertà delle persone fisiche in ordine al trattamento dei dati personali, tutti i processi, inclusi i procedimenti amministrativi di competenza del titolare, vanno gestiti conformemente alle disposizioni del Codice, del RGPD, e del presente Regolamento.
4. Il presente Regolamento tiene conto dei seguenti documenti:
   a) Codice in materia di dati personali (D.lgs. n.196/2003);
   b) Linee guida e raccomandazioni del Garante;
   c) RGPD UE 679/2016 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE;
   d) Legge 25 ottobre 2017, n. 163 (art.13), recante la delega per l'adeguamento della normativa nazionale alle disposizioni del RGPD (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE;
   e) D.lgs. n. 101/2018 di adeguamento della normativa interna al RGPD;
   f) Dichiarazioni del gruppo di lavoro articolo 29 sulla protezione dei dati (WP29) - 14/EN;
   g) Linee-guida sui responsabili della protezione dei dati (RPD) - WP243 Adottate dal Gruppo di lavoro Art. 29 il 13 dicembre 2016;
   h) Linee-guida sul diritto alla "portabilità dei dati" - WP242 Adottate dal Gruppo di lavoro Art. 29 il 13 dicembre 2016;
   i) Linee-guida per l'individuazione dell'autorità di controllo capofila in rapporto a uno specifico Titolare o Responsabile del trattamento - WP244 adottate dal Gruppo di lavoro Art. 29 il 13 dicembre 2016;
   j) Linee-guida concernenti la valutazione di impatto sulla protezione dei dati nonché i criteri per stabilire se un trattamento "possa presentare un rischio elevato" ai sensi del regolamento 2016/679 - WP248 adottate dal Gruppo di lavoro Art. 29 il 4 aprile 2017;
   k) Linee guida elaborate dal Gruppo Art. 29 in materia di applicazione e definizione delle sanzioni amministrative - WP253 adottate dal Gruppo di lavoro Art. 29 il 3 ottobre 2017;

l) Linee guida elaborate dal Gruppo Art. 29 in materia di processi decisionali automatizzati e profilazione - WP251 Adottate dal Gruppo di lavoro Art. 29 il 6 febbraio 2018;
m) Linee guida elaborate dal Gruppo Art. 29 in materia di notifica delle violazioni di dati personali (data breach notification) - WP250 Adottate dal Gruppo di lavoro Art. 29 il 6 febbraio 2018;
n) Parere del WP29 sulla limitazione della finalità - 13/EN WP 203;
o) Norme internazionali relative alla Protezione dei Dati Personali;
p) Regolamenti interni, approvati dai titolari e/o dai responsabili.
q) l'art. 88, comma 2, lett. f) del CCNL Scuola del 29 novembre 2007
r) la legge 107/2015 all'art. 1 comma 83

Art. 2
Principi e responsabilizzazione

Vengono integralmente recepiti, nell'ordinamento interno del titolare, i principi del RGPD, per effetto dei quali i dati personali sono:

a) trattati in modo lecito, corretto e trasparente nei confronti dell'interessato ("liceità, correttezza e trasparenza");
b) raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità; un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è considerato incompatibile con le finalità iniziali ("limitazione della finalità");
c) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati base del principio di "minimizzazione dei dati";
d) esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati base del principio di "esattezza";
e) conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1 RGPD, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle libertà dell'interessato in base al principio di "limitazione della conservazione";
f) trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali in base ai principi di "integrità e riservatezza";
g) configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalità possano essere perseguite mediante dati anonimi o con l'uso di opportune modalità che permettono di identificare l'interessato solo un caso di necessità *("principio di necessità*").

Il titolare è competente per il rispetto dei principi sopra declinati, ed è in grado di comprovarlo in base al principio di *accountability*.

Art. 3
Liceità del trattamento

Vengono integralmente recepiti, nell'ordinamento interno del titolare, le disposizioni del RGPD in ordine alla liceità del trattamento e, per l'effetto, il trattamento è lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni:

a) l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità;
b) il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso;
c) il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il Titolare del trattamento;
d) il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica;
e) il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il Titolare del trattamento.
f) il trattamento è necessario per il perseguimento del legittimo interesse del Titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore.

La lettera f) non si applica al trattamento di dati effettuato dal titolare nell'esecuzione dei propri compiti e funzioni.

Laddove il trattamento per una finalità diversa da quella per la quale i dati personali sono stati raccolti non sia basato sul consenso dell'interessato o su un atto legislativo dell'Unione o degli Stati membri che costituisca una misura necessaria e proporzionata per la salvaguardia degli obiettivi di cui all'articolo 23, paragrafo 1 RGPD, al fine di verificare se il trattamento per un'altra finalità sia compatibile con la finalità per la quale i dati personali sono stati inizialmente raccolti, il Titolare tiene conto, tra l'altro:
a) di ogni nesso tra le finalità per cui i dati personali sono stati raccolti e le finalità dell'ulteriore trattamento previsto;
b) del contesto in cui i dati personali sono stati raccolti, in particolare relativamente alla relazione tra l'interessato e il Titolare del trattamento;
c) della natura dei dati personali, specialmente se siano trattate categorie particolari di dati personali ai sensi dell'art. 9 del RGPD, oppure se siano trattati dati relativi a condanne penali e a reati ai sensi dell'articolo 10 del medesimo RGPD;
d) delle possibili conseguenze dell'ulteriore trattamento previsto per gli interessati;
e) dell'esistenza di garanzie adeguate, che possono comprendere la cifratura o la pseudonimizzazione.

Art. 4
Informativa

Il titolare, precedentemente all'inizio delle procedure di Trattamento dei dati personali o comunque al primo istante utile successivamente allo stesso, è tenuto a fornire all'interessato, anche avvalendosi del personale incaricato, apposita informativa secondo le modalità previste dagli Artt. 13 e 14 RGPD, in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro, in particolare nel caso di informazioni destinate specificamente ai minori.
L'informativa è data, in linea di principio, per iscritto e preferibilmente in formato elettronico, soprattutto nel contesto di servizi online, anche se sono ammessi altri mezzi, potendo essere fornita anche oralmente, ma nel rispetto delle caratteristiche di cui sopra. L'informativa è fornita, mediante idonei strumenti:

- attraverso appositi moduli da consegnare agli interessati. Nel modulo sono indicati i soggetti a cui l'utente può rivolgersi per ottenere maggiori informazioni ed esercitare i propri diritti, anche al fine di consultare l'elenco aggiornato dei responsabili;

- avvisi agevolmente visibili dal pubblico, posti nei locali di accesso delle strutture del titolare, nelle sale d'attesa e in altri locali in cui ha accesso l'utenza o diffusi nell'ambito di pubblicazioni istituzionali e mediante il sito internet del titolare;
- apposita avvertenza inserita nei contratti ovvero nelle lettere di affidamento di incarichi del personale dipendente, dei soggetti con i quali vengono instaurati rapporti di collaborazione o libero-professionali, dei tirocinanti, dei volontari, degli stagisti ed altri soggetti che entrano in rapporto con il titolare.;
- resa in sede di pubblicazione dei bandi, avvisi, lettere d'invito, con l'indicazione dell'incaricato del trattamento dei dati relativi alle procedure.

L'informativa da fornire agli interessati può essere fornita anche in combinazione con icone standardizzate per dare, in modo facilmente visibile, intelligibile e chiaramente leggibile, un quadro d'insieme del trattamento previsto. Se presentate elettronicamente, le icone sono leggibili da dispositivo automatico.
L'informativa contiene il seguente contenuto minimo:

- l'identità e dati di contatto del titolare e, ove presente, del suo rappresentante;
- i dati di contatto del RPD/DPO ove esistente;
- le finalità del trattamento;
- i destinatari dei dati;
- la base giuridica del trattamento;
- l'interesse legittimo del titolare se quest'ultimo costituisce la base giuridica del trattamento;
- se il titolare trasferisce i dati personali in Paesi terzi e, in caso affermativo, attraverso quali strumenti;
- il periodo di conservazione dei dati o i criteri seguiti per stabilire tale periodo di conservazione;
- il diritto dell'interessato di chiedere al titolare l'accesso, la rettifica, la cancellazione dei dati, la limitazione del trattamento che lo riguarda, il diritto di opporsi al trattamento e il diritto alla portabilità dei dati;
- il diritto di presentare un reclamo all'autorità di controllo;
- l'esistenza di un processo decisionale automatizzato, compresa la profilazione, e le informazioni significative sulla logica utilizzata nonché l'importanza e le conseguenze di tale trattamento per l'interessato.

Nel caso di dati personali non raccolti direttamente presso l'interessato:

a) il titolare deve informare l'interessato in merito a:
   - le categorie di dati personali trattati;
   - la fonte da cui hanno origine i dati personali e l'eventualità che i dati provengano da fonti accessibili al pubblico.
b) l'informativa deve essere fornita entro un termine ragionevole che non può superare 1 mese dalla raccolta, oppure dal momento della comunicazione (e non della registrazione) dei dati a terzi o all'interessato.

Un' informativa generale deve essere fornita alle famiglie in occasione delle iscrizioni relativamente ai trattamenti di dati personali operati dalla scuola per il conseguimento delle proprie finalità istituzionali.
Per i trattamenti dei dati connessi alla gestione del rapporto di lavoro con il personale dipendente del titolare è predisposta apposita informativa per personale dipendente.
Apposite informative devono essere inserite nei seguenti documenti:

- nei bandi e nella documentazione di affidamento dei contratti pubblici;
- nei contratti, accordi o convenzioni;
- nei bandi di concorso pubblico;

– nelle segnalazioni di disservizio e, più in generale, in ogni altro documento contenente dati personali.

Nel fornire l'informativa, il titolare fa espresso riferimento alla normativa che prevede gli obblighi o i compiti in base alla quale è effettuato il trattamento dei dati sensibili e giudiziari.

Art. 5
Informativa per utilizzo di sistemi di videosorveglianza

1. Nel caso di utilizzo di sistemi di videosorveglianza per finalità di sicurezza degli edifici, gli interessati devono essere sempre informati che stanno per accedere in una zona videosorvegliata; ciò anche nei casi di eventi e in occasione di spettacoli pubblici (es. concerti, manifestazioni sportive).
2. A tal fine può essere utilizzato un modello di informativa semplificata che poi rinvii a un testo contenente tutti gli elementi completi di cui all'articolo precedente, disponibile agevolmente senza oneri per gli interessati, sia sul sito internet dell'amministrazione.
3. In ogni caso il Titolare, anche per il tramite di un incaricato, ove richiesto è tenuto a fornire anche oralmente un'informativa adeguata, contenente gli elementi individuati dall'articolo precedente.
4. Il supporto con l'informativa:

- deve essere collocato prima del raggio di azione della telecamera, anche nelle sue immediate vicinanze e non necessariamente a contatto con gli impianti;
- deve avere un formato ed un posizionamento tale da essere chiaramente visibile in ogni condizione di illuminazione ambientale, anche quando il sistema di videosorveglianza sia eventualmente attivo in orario notturno;
- può inglobare un simbolo o una stilizzazione di esplicita e immediata comprensione, eventualmente diversificati al fine di informare se le immagini sono solo visionate o anche registrate.

Art. 6
Sensibilizzazione e formazione

Ai fini della corretta e puntuale applicazione della disciplina relativa ai principi, alla liceità del trattamento, al consenso, all'informativa e, più in generale, alla protezione dei dati personali, il titolare sostiene e promuove, all'interno della propria struttura organizzativa, ogni strumento di sensibilizzazione che possa consolidare la consapevolezza del valore della riservatezza dei dati, e migliorare la qualità del servizio.
A tale riguardo, il presente regolamento riconosce che uno degli strumenti essenziali di sensibilizzazione è l'attività formativa del personale del titolare e l'attività informativa diretta a tutti coloro che hanno rapporti con il titolare.
Per garantire la conoscenza capillare delle disposizioni del presente Regolamento, al momento dell'ingresso in servizio è data a ogni dipendente una specifica comunicazione, con apposita clausola inserita nel contratto di lavoro, contenente tutti i principi fondamentali della materia, esposti in maniera semplice, chiara e puntuale, con i riferimenti per l'acquisizione del presente Regolamento, pubblicato sul sito del Titolare. Il dipendente si impegna ad acquisire copia del Regolamento, prenderne visione ed attenersi alle sue prescrizioni.
Il titolare organizza, nell'ambito della formazione continua e obbligatoria del personale, specifici interventi di formazione e di aggiornamento, anche integrati con gli interventi di formazione anticorruzione, in materia di protezione dei dati personali, finalizzati alla conoscenza delle norme, alla prevenzione di fenomeni di abuso e illegalità nell'attuazione della normativa, all'adozione di idonei modelli di comportamento e procedure di trattamento, alla conoscenza delle misure di sicurezza per il trattamento e la conservazione dei dati, dei rischi individuati e dei modi per prevenire danni agli interessati.

La formazione in materia di prevenzione dei rischi di violazione dei dati personali viene integrata e coordinata, a cura del RPC, con la formazione in materia di prevenzione della corruzione e della illegalità nonché con la formazione in tema di trasparenza e di accesso, con particolare riguardo ai rapporti tra protezione dei dati personali, trasparenza accesso ai documenti amministrativi e accesso civico, semplice e generalizzato, nei diversi ambiti in cui opera il titolare.
L'attività di formazione del personale dovrà essere documentata nel registro della formazione tenuto dall'istituto.

TITOLO II
IL TRATTAMENTO DEI DATI PERSONALI

Art. 7
Trattamenti operati e personale autorizzato

Il titolare tratta i dati personali per lo svolgimento delle proprie finalità istituzionali, come identificate da disposizioni di legge, statutarie e regolamentari, e nei limiti imposti dal Codice, dal RGPD e dalle Linee guida e dai provvedimenti del Garante.
Il titolare effettua i trattamenti di dati personali, previsti da disposizioni legislative e regolamentari riguardanti, a titolo esemplificativo e non esaustivo:

- Per la gestione delle attività didattico-formative e di valutazione comprese quelle propedeutiche all'avvio dell'ano scolastico, quelle socio-assistenziali e qualunque altra prevista nel Piano Triennale dell'Offerta Formativa
- Per la gestione del personale dipendente, ivi comprese le procedure di assunzione; la gestione dei soggetti che intrattengono rapporti giuridici con il titolare, diversi dal rapporto di lavoro dipendente, e che operano a qualsiasi titolo all'interno della struttura organizzativa del titolare, ivi compresi gli stagisti, tirocinanti e i volontari;
- Per la gestione dei rapporti con i consulenti, i libero-professionisti, i fornitori per l'approvvigionamento di beni e di servizi nonché con le imprese per l'esecuzione lavori, opere e di interventi di manutenzione;
- Per la gestione dei rapporti con i soggetti accreditati o convenzionati per i servizi socio-assistenziali;
- Per la gestione dei rapporti con la Procura della Repubblica e gli altri soggetti pubblici competenti, per le attività ispettive di vigilanza, di controllo e di accertamento delle infrazioni alle leggi e regolamenti.

Il trattamento dei dati personali è esercitabile, all'interno della struttura organizzativa del titolare, solo da parte dei soggetti appositamente autorizzati. A tal fine il dirigente scolastico, titolare del trattamento, ha istituito le seguenti unità organizzative autorizzate al trattamento cui deve essere assegnato tutto il personale in servizio:

- Personale docente
- Personale amministrativo
- Assistenti tecnici
- Collaboratori scolastici
- D.S.G.A.
- Funzioni Strumentali

Art. 8
Registro delle attività di trattamento

Il titolare del trattamento istituisce un registro, in forma scritta, delle attività di trattamento e delle categorie di trattamenti svolte sotto la propria responsabilità.
Il registro deve essere continuamente aggiornato e messo a disposizione delle autorità di controllo.

Tale registro contiene le seguenti informazioni:

- il nome e i dati di contatto del Titolare del trattamento, del Responsabile per la protezione dei dati, dei responsabili e degli incaricati;
- le finalità del trattamento;
- una descrizione delle categorie di interessati e delle categorie dei dati personali;
- le categorie dei trattamenti effettuati;
- le categorie di destinatari, a cui i dati personali sono o saranno comunicati;
- l'indicazione delle cautele specifiche, a cui ciascun Responsabile deve attendere in modo che siano appropriate rispetto ai trattamenti verso cui dovrà rispondere;
- un'eventuale possibilità di trasferimenti di dati all'estero;
- una descrizione generale delle misure di sicurezza, generiche e specifiche, così come disciplinate dalla normativa vigente in tema di sicurezza dei dati personali;
- indicazione dei termini ultimi previsti per la cancellazione delle diverse categorie di dati trattati;
- un elenco dei processi di trattamento effettuati da ciascuna area funzionale dell'istituto.

Il responsabile di trattamento tiene registro di tutte le categorie di attività relative al trattamento svolte per conto di un titolare del trattamento, contenente:

a) il nome e i dati di contatto del responsabile o dei responsabili del trattamento, di ogni titolare del trattamento per conto del quale agisce il responsabile del trattamento, del rappresentante del titolare del trattamento o del responsabile del trattamento e, ove applicabile, del responsabile della protezione dei dati;
b) le categorie dei trattamenti effettuati per conto di ogni titolare del trattamento;
c) ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'articolo 49, la documentazione delle garanzie adeguate;
d) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, paragrafo 1 RGPD

I registri sono tenuti in forma scritta, anche in formato elettronico.
Su richiesta, il titolare del trattamento o il responsabile del trattamento, mettono il registro a disposizione del Garante. Il presente documento costituisce integrazione e completamento del registro dei trattamenti.

Art. 9
Tipologie di dati trattati

Nell'ambito dei trattamenti inclusi nell'indice dei trattamenti, il titolare, nell'esercizio delle sue funzioni istituzionali, tratta in modo anche automatizzato, totalmente o parzialmente, le seguenti tipologie di dati:

- dati comuni identificativi
- dati ex Art. 9 RGPD
- dati ex Art. 10 RGPD

Art. 10
Trattamento dei dati ex Art. 9 RGPD

Il titolare conforma il trattamento dei Dati Personali "particolari" ex Art. 9 RGPD secondo modalità volte a prevenire violazioni dei diritti, delle libertà fondamentali e della dignità dell'interessato. A tale fine, il titolare applica i principi del succitato articolo, e si conforma alle Linee Guida del Garante in materia. In particolare:

1. È vietato trattare dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.
2. Il paragrafo 1 non si applica se si verifica uno dei seguenti casi:
   a) l'interessato ha prestato il proprio consenso esplicito al trattamento di tali dati personali per una o più finalità specifiche, salvo nei casi in cui il diritto dell'Unione o degli Stati membri dispone che l'interessato non possa revocare il divieto di cui al paragrafo 1;
   b) il trattamento è necessario per assolvere gli obblighi ed esercitare i diritti specifici del titolare del trattamento o dell'interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale, nella misura in cui sia autorizzato dal diritto dell'Unione o degli Stati membri o da un contratto collettivo ai sensi del diritto degli Stati membri, in presenza di garanzie appropriate per i diritti fondamentali e gli interessi dell'interessato;
   c) il trattamento è necessario per tutelare un interesse vitale dell'interessato o di un'altra persona fisica qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso;
   d) il trattamento è effettuato, nell'ambito delle sue legittime attività e con adeguate garanzie, da una fondazione, associazione o altro organismo senza scopo di lucro che persegua finalità politiche, filosofiche, religiose o sindacali, a condizione che il trattamento riguardi unicamente i membri, gli ex membri o le persone che hanno regolari contatti con la fondazione, l'associazione o l'organismo a motivo delle sue finalità e che i dati personali non siano comunicati all'esterno senza il consenso dell'interessato;
   e) il trattamento riguarda dati personali resi manifestamente pubblici dall'interessato;
   f) il trattamento è necessario per accertare, esercitare o difendere un diritto in sede giudiziaria o ogniqualvolta le autorità giurisdizionali esercitino le loro funzioni giurisdizionali;
   g) il trattamento è necessario per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri, che deve essere proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato;
   h) il trattamento è necessario per finalità di medicina preventiva o di medicina del lavoro, valutazione della capacità lavorativa del dipendente, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali sulla base del diritto dell'Unione o degli Stati membri o conformemente al contratto con un professionista della sanità, fatte salve le condizioni e le garanzie di cui al paragrafo 3;
   i) il trattamento è necessario per motivi di interesse pubblico nel settore della sanità pubblica, quali la protezione da gravi minacce per la salute a carattere transfrontaliero o la garanzia di parametri elevati di qualità e sicurezza dell'assistenza sanitaria e dei medicinali e dei dispositivi medici, sulla base del diritto dell'Unione o degli Stati membri che prevede misure appropriate e specifiche per tutelare i diritti e le libertà dell'interessato, in particolare il segreto professionale;
   j) il trattamento è necessario a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici in conformità dell'articolo 89, paragrafo 1, sulla base del diritto dell'Unione o nazionale, che è proporzionato alla finalità perseguita, rispetta l'essenza del diritto alla protezione dei dati e prevede misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato.

Il trattamento dei dati sensibili e giudiziari dovrà avvenire nel rispetto del Decreto 7 dicembre 2006, n. 305 del Ministero dell'Istruzione dal titolo *"Regolamento recante identificazione dei dati sensibili e giudiziari trattati e delle relative operazioni effettuate dal Ministero della pubblica istruzione, in attuazione degli articoli 20 e 21 del decreto legislativo 30 giugno 2003, n. 196, recante «Codice in materia di protezione dei dati personali»"*

Il titolare sensibilizza, forma e aggiorna i dipendenti in ordine al trattamento di questa tipologia di dati personali.

Art. 11
Trattamento di categorie particolari di dati personali necessario per motivi di interesse pubblico rilevante

1. I presupposti di liceità di cui all'Art 9, comma g) del presente regolamento sono regolati dall'Art. 2-sexies del Codice Privacy.
2. I trattamenti delle categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, del RGPD, necessari per motivi di interesse pubblico rilevante ai sensi del paragrafo 2, lettera g), del medesimo articolo, sono ammessi qualora siano previsti dal diritto dell'Unione europea ovvero, nell'ordinamento interno, da disposizioni di legge o, nei casi previsti dalla legge, di regolamento o da atti amministrativi generali che specifichino i tipi di dati che possono essere trattati, le operazioni eseguibili e il motivo di interesse pubblico rilevante, nonché le misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato.
3. Fermo quanto previsto dal comma 2, si considera rilevante l'interesse pubblico relativo a trattamenti effettuati da soggetti che svolgono compiti di interesse pubblico o connessi all'esercizio di pubblici poteri nelle seguenti materie:
   a) accesso a documenti amministrativi e accesso civico;
   b) tenuta degli atti e dei registri dello stato civile, delle anagrafi della popolazione residente in Italia e dei cittadini italiani residenti all'estero, e delle liste elettorali, nonché rilascio di documenti di riconoscimento o di viaggio o cambiamento delle generalità;
   c) tenuta di registri pubblici relativi a beni immobili o mobili;
   d) tenuta dell'anagrafe nazionale degli abilitati alla guida e dell'archivio nazionale dei veicoli;
   e) cittadinanza, immigrazione, asilo, condizione dello straniero e del profugo, stato di rifugiato;
   f) elettorato attivo e passivo ed esercizio di altri diritti politici, protezione diplomatica e consolare, nonché documentazione delle attività istituzionali di organi pubblici, con particolare riguardo alla redazione di verbali e resoconti dell'attività di assemblee rappresentative, commissioni e di altri organi collegiali o assembleari;
   g) esercizio del mandato degli organi rappresentativi, ivi compresa la loro sospensione o il loro scioglimento, nonché l'accertamento delle cause di ineleggibilità, incompatibilità o di decadenza, ovvero di rimozione o sospensione da cariche pubbliche;
   h) svolgimento delle funzioni di controllo, indirizzo politico, inchiesta parlamentare o sindacato ispettivo e l'accesso a documenti riconosciuto dalla legge e dai regolamenti degli organi interessati per esclusive finalità direttamente connesse all'espletamento di un mandato elettivo;
   i) attività dei soggetti pubblici dirette all'applicazione, anche tramite i loro concessionari, delle disposizioni in materia tributaria e doganale;
   j) attività di controllo e ispettive;
   k) concessione, liquidazione, modifica e revoca di benefici economici, agevolazioni, elargizioni, altri emolumenti e abilitazioni;
   l) conferimento di onorificenze e ricompense, riconoscimento della personalità giuridica di associazioni, fondazioni ed enti, anche di culto, accertamento dei requisiti di onorabilità e di professionalità per le nomine, per i profili di competenza del soggetto pubblico, ad uffici anche di culto e a cariche direttive di persone giuridiche, imprese e di istituzioni scolastiche non statali, nonché rilascio e revoca di autorizzazioni o abilitazioni, concessione di patrocini, patronati e premi di rappresentanza, adesione a comitati d'onore e ammissione a cerimonie ed incontri istituzionali;
   m) rapporti tra i soggetti pubblici e gli enti del terzo settore;
   n) obiezione di coscienza;

o) attività sanzionatorie e di tutela in sede amministrativa o giudiziaria;
p) rapporti istituzionali con enti di culto, confessioni religiose e comunità religiose;
q) attività socio-assistenziali a tutela dei minori e soggetti bisognosi, non autosufficienti e incapaci;
r) attività amministrative e certificatorie correlate a quelle di diagnosi, assistenza o terapia sanitaria o sociale, ivi incluse quelle correlate ai trapianti d'organo e di tessuti nonché alle trasfusioni di sangue umano;
s) compiti del servizio sanitario nazionale e dei soggetti operanti in ambito sanitario, nonché compiti di igiene e sicurezza sui luoghi di lavoro e sicurezza e salute della popolazione, protezione civile, salvaguardia della vita e incolumità fisica;
t) programmazione, gestione, controllo e valutazione dell'assistenza sanitaria, ivi incluse l'instaurazione, la gestione, la pianificazione e il controllo dei rapporti tra l'amministrazione ed i soggetti accreditati o convenzionati con il servizio sanitario nazionale;
u) vigilanza sulle sperimentazioni, farmacovigilanza, autorizzazione all'immissione in commercio e all'importazione di medicinali e di altri prodotti di rilevanza sanitaria;
v) tutela sociale della maternità ed interruzione volontaria della gravidanza, dipendenze, assistenza, integrazione sociale e diritti dei disabili;
w) istruzione e formazione in ambito scolastico, professionale, superiore o universitario;
x) trattamenti effettuati a fini di archiviazione nel pubblico interesse o di ricerca storica, concernenti la conservazione, l'ordinamento e la comunicazione dei documenti detenuti negli archivi di Stato negli archivi storici degli enti pubblici, o in archivi privati dichiarati di interesse storico particolarmente importante, per fini di ricerca scientifica, nonché per fini statistici da parte di soggetti che fanno parte del sistema statistico nazionale (Sistan);
y) instaurazione, gestione ed estinzione, di rapporti di lavoro di qualunque tipo, anche non retribuito o onorario, e di altre forme di impiego, materia sindacale, occupazione e collocamento obbligatorio, previdenza e assistenza, tutela delle minoranze e pari opportunità nell'ambito dei rapporti di lavoro, adempimento degli obblighi retributivi, fiscali e contabili, igiene e sicurezza del lavoro o di sicurezza o salute della popolazione, accertamento della responsabilità civile, disciplinare e contabile, attività ispettiva.

4. Per i dati genetici, biometrici e relativi alla salute il trattamento avviene comunque nel rispetto di quanto previsto dall'articolo 2-*septies* del Codice Privacy.

Art. 12
Trattamento dei dati del personale

Il titolare tratta i dati, anche ex Art. 9 o 10 RGPD, dei propri dipendenti per le finalità, considerate di rilevante interesse pubblico, di instaurazione e di gestione di rapporti di lavoro di qualunque tipo.
Tra tali trattamenti sono compresi quelli effettuati al fine di accertare il possesso di particolari requisiti previsti per l'accesso a specifici impieghi, la sussistenza dei presupposti per la sospensione o la cessazione dall'impiego o dal servizio, di adempiere agli obblighi connessi alla definizione dello stato giuridico od economico del personale, nonché ai relativi obblighi retributivi, fiscali e contabili, relativamente al personale in servizio o in quiescenza.
Secondo la normativa vigente, il titolare adotta le massime cautele nel trattamento di informazioni personali del proprio personale dipendente che siano idonee a rivelare lo stato di salute, le abitudini sessuali, le convinzioni politiche, sindacali, religiose filosofiche o d'altro genere e l'origine razziale ed etnica.
Il trattamento dei dati sensibili del dipendente, da parte del datore di lavoro, deve avvenire secondo i principi di necessità e di indispensabilità che impongono di ridurre al minimo l'utilizzo dei dati personali, e quando non si possa prescindere dall'utilizzo dei dati giudiziari e sensibili, di trattare solo le informazioni che si rivelino indispensabili per la gestione del rapporto di lavoro.

La pubblicazione delle graduatorie di selezione del personale o relative alla concessione, liquidazione, modifica e revoca di benefici economici, agevolazioni, elargizioni, deve essere effettuata dopo un'attenta verifica che le indicazioni contenute non comportino la divulgazione di dati idonei a rivelare lo stato di salute, utilizzando diciture generiche o codici numerici.
Non sono infatti ostensibili, se non nei casi previsti dalla legge, le notizie concernenti la natura delle infermità e degli impedimenti personali o familiari che causino l'astensione del lavoro, nonché le componenti della valutazione o le notizie concernenti il rapporto di lavoro tra il personale dipendente e l'amministrazione, idonee a rivelare taluna delle informazioni di natura sensibile.
Il titolare, nel trattamento dei dati sensibili relativi alla salute dei propri dipendenti, deve rispettare i principi di necessità e indispensabilità.
Il titolare si conforma alle Linee Guida del Garante in materia di trattamento dei dati personali dei lavoratori per finalità di gestione del rapporto di lavoro in ambito pubblico.

Art. 13
Pubblicazione web per obblighi di pubblicità legale e trasparenza

1. L'Istituto effettua il trattamento di dati personali, contenuti in atti e documenti amministrativi, che devono essere pubblicati all'albo on line per obblighi di pubblicità legale ed in Amministrazione Trasparente per obblighi di trasparenza previsti dal D.Lgs. n. 33/2013.
2. I documenti di cui al comma 1 sono pubblicati tempestivamente sul sito istituzionale dell'amministrazione e vanno mantenuti aggiornati.
3. Non possono essere resi intelligibili i dati non necessari, eccedenti o non pertinenti con la finalità di pubblicazione.
4. I dati particolari idonei a rivelare origine razziale ed etnica, convinzioni religiose, filosofiche o di altro genere, opinioni politiche, adesione a partiti, sindacati, associazioni e organizzazioni a carattere filosofico, politico o sindacale possono essere diffusi solo se indispensabili; i dati particolari relativi alla vita sessuale non possono essere diffusi per finalità di trasparenza, fatto salvo quanto previsto dall'Art. 9, comma 2 g) del presente regolamento. Qualora si rendesse necessario un trattamento dati di questo tipo, è necessario richiedere il parere del RPC e del RPD preventivamente all'inizio delle attività di trattamento.
5. I dati particolari idonei a rivelare lo stato di salute non devono essere diffusi.
6. I dati vanno pubblicati in formato di tipo aperto ai sensi dell'art. 68, D.Lgs. n. 82/2005 e sono liberamente riutilizzabili secondo la normativa vigente.
7. I dati personali diversi dai dati sensibili e dai dati giudiziari devono essere pubblicati all'albo on line per il tempo necessario ad assolvere agli obblighi di pubblicità legale (di norma 15 giorni se non previsto esplicitamente altro termine). I dati ed i documenti pubblicati all'albo non possono essere oggetto di indicizzazione da parte dei motori di ricerca.
8. I dati personali diversi dai dati sensibili e dai dati giudiziari devono essere pubblicati in amministrazione trasparente per assolvere agli obblighi di pubblicità legale previsti dal D.Lgs 33/2013. I dati ed i documenti pubblicati all'albo devono consentire l'indicizzazione e la rintracciabilità tramite i motori di ricerca web.
9. I dati, le informazioni e i documenti di cui al comma 8, sono pubblicati per un periodo di 5 anni, decorrenti dal 1° gennaio dell'anno successivo a quello dell'obbligo di pubblicazione.
10. Deroghe alla predetta durata temporale quinquennale sono previste:
    a) nel caso in cui gli atti producono ancora i loro effetti alla scadenza dei cinque anni, con la conseguenza che gli stessi devono rimanere pubblicati fino alla cessazione della produzione degli effetti;
    b) per alcuni dati e informazioni riguardanti i titolari di incarichi politici, di carattere elettivo o comunque di esercizio di poteri di indirizzo politico, di livello statale regionale e locale ai sensi dell'art. 14, comma 2, D.Lgs. n. 33/2013 e i titolari di incarichi dirigenziali e di

collaborazione o consulenza che devono rimanere pubblicati online per i tre anni successivi dalla cessazione del mandato o dell'incarico ai sensi dell'art. 15, comma 4, D.Lgs. n. 33/2013;

c) nel caso in cui siano previsti diversi termini dalla normativa in materia di trattamento dei dati personali.

11. I dati personali devono essere conservati, in ogni caso, per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati; l'interessato ha sempre diritto di ottenere la cancellazione dei dati personali di cui non è necessaria la conservazione in relazione agli scopi per i quali sono stati raccolti o successivamente trattati.
12. Il titolare si impegna a emanare delle linee guida specifiche relative alla pubblicazione di documenti amministrativi sull'Albo Online ed in Amministrazione Trasparente, quali allegati tecnici al presente documento.

Art. 14
Trattamento dei dati personali effettuato con sistemi di videosorveglianza

1. Il trattamento dei dati personali effettuato mediante l'uso di sistemi di videosorveglianza richiede apposita informativa agli interessati e questa può essere rilasciata in forma semplificata come indicato all'Art. 5.
2. Per finalità di tutela della sicurezza urbana, la durata della conservazione dei dati è limitata *"ai* sette giorni successivi[1] alla rilevazione delle informazioni e delle immagini raccolte mediante l'uso di sistemi di videosorveglianza, fatte salve speciali esigenze di ulteriore conservazione in conformità dell'art. 6, co. 9, D.L. n. 11/2009. Tempi di durata maggiore della conservazione dei dati necessitano una specifica valutazione dei rischi, motivata con riferimento ad una specifica esigenza di sicurezza perseguita, in relazione a concrete situazioni di rischio riguardanti eventi realmente incombenti (es. collaborazione con l'autorità giudiziaria o dalla polizia giudiziaria in relazione ad un'attività investigativa in corso).

[1] Cfr. Garante privacy, Provvedimento 8 aprile 2010, n. 1712680, par. 3.4. Negli altri casi i tempi di conservazione sono 24 ore dalla rilevazione dei dati.

TITOLO III
DIRITTI DEGLI INTERESSATI

Art. 15
Diritto di accesso alla documentazione, diritto di accesso civico e protezione dei dati personali

I presupposti, le modalità, i limiti per l'esercizio del diritto di accesso ai documenti amministrativi e del diritto di accesso civico, semplice e generalizzato, contenenti dati personali, e la relativa tutela giurisdizionale, restano disciplinati dalla normativa in materia di accesso agli atti e di accesso civico, anche per ciò che concerne i tipi di dati sensibili e giudiziari, e le operazioni di trattamento eseguibili in esecuzione di una richiesta di accesso.
Le attività finalizzate all'applicazione di tale disciplina si considerano di rilevante interesse pubblico.
Il titolare si conforma alle Linee guida del Garante in tema di rapporti tra accesso alla documentazione, diritto di accesso civico e protezione dei dati personali.
Il titolare si impegna a emanare delle linee guida specifiche relative alla gestione delle richieste di accesso civico e documentale.

Art. 16
Diritti dell'interessato

Il titolare attua e implementa le misure organizzative, gestionali, procedurali e documentali necessarie a facilitare l'esercizio dei diritti dell'interessato, di seguito elencati, in conformità alla disciplina contenuta nel RGPD e nel Codice.

Art. 17
Diritto di accesso

Il presente Regolamento tiene conto della disciplina del RGPD in tema di diritto di accesso secondo la quale l'interessato ha il diritto di ottenere dal titolare del trattamento la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e in tal caso, di ottenere l'accesso ai dati personali e alle seguenti informazioni:

a) le finalità del trattamento;
b) le categorie di dati personali in questione;
c) i destinatari o le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, in particolare se destinatari di paesi terzi o organizzazioni internazionali;
d) quando possibile, il periodo di conservazione dei dati personali previsto oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
e) l'esistenza del diritto dell'interessato di chiedere al Titolare del trattamento la rettifica o la cancellazione dei dati personali o la limitazione del trattamento dei dati personali che lo riguardano o di opporsi al loro trattamento;
f) il diritto di proporre reclamo a un'autorità di controllo;
g) qualora i dati non siano raccolti presso l'interessato, tutte le informazioni disponibili sulla loro origine;
h) l'esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'articolo 22, paragrafi 1 e 4 RGPD, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.

Qualora i dati personali siano trasferiti a un paese terzo o a un'organizzazione internazionale, l'interessato ha il diritto di essere informato dell'esistenza di garanzie adeguate.
Il titolare del trattamento fornisce una copia dei dati personali oggetto di trattamento. In caso di ulteriori copie richieste dall'interessato, il titolare del trattamento può addebitare un contributo spese ragionevole basato sui costi amministrativi effettivamente affrontati.
Se l'interessato presenta la richiesta mediante mezzi elettronici, e salvo indicazione diversa dell'interessato, le informazioni sono fornite in un formato elettronico di uso comune.
Il diritto di ottenere una copia non deve ledere i diritti e le libertà altrui.

Art. 18
Diritto alla rettifica e cancellazione

Il presente Regolamento tiene conto della disciplina del RGPD in tema di diritto di rettifica e cancellazione ("diritto all'oblio"), di seguito indicata.
Quanto al diritto di rettifica, l'interessato ha il diritto di ottenere dal titolare del trattamento la rettifica dei dati personali inesatti che lo riguardano senza ingiustificato ritardo. Tenuto conto delle finalità del trattamento, l'interessato ha il diritto di ottenere l'integrazione dei dati personali incompleti, anche fornendo una dichiarazione integrativa.
Il titolare comunica a ciascuno dei destinatari cui sono stati trasmessi i dati personali le eventuali rettifiche, salvo che ciò si riveli impossibile o implichi uno sforzo sproporzionato.
Quanto al diritto "all'oblio", consistente nel diritto di ottenere dal titolare del trattamento la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo, lo stesso non si applica nella misura in cui il trattamento sia necessario:

- per l'esercizio del diritto alla libertà di espressione e di informazione;
- per l'adempimento di un obbligo legale che richieda il trattamento previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento o per l'esecuzione di un compito svolto nel pubblico interesse oppure nell'esercizio di pubblici poteri di cui è investito il titolare del trattamento;
- per motivi di interesse pubblico nel settore della sanità pubblica in conformità dell'articolo 9, paragrafo 2, lettere h) e i), e dell'articolo 9, paragrafo 3 RGPD;
- a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici conformemente all'articolo 89, paragrafo 1 RGPD, nella misura in cui il diritto all'oblio rischi di rendere impossibile o di pregiudicare gravemente il conseguimento degli obiettivi di tale trattamento;
- per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.

Art. 19
Diritto alla limitazione

Il presente Regolamento tiene conto della disciplina del RGPD in tema di diritto alla limitazione, e di seguito indicata.
L'interessato ha il diritto di ottenere dal titolare la limitazione del trattamento quando ricorre una delle seguenti condizioni:

a) l'interessato contesta l'esattezza dei dati personali, per il periodo necessario al titolare per verificare l'esattezza di tali dati personali;
b) il trattamento è illecito e l'interessato si oppone alla cancellazione dei dati personali e chiede invece che ne sia limitato l'utilizzo;

c) benché il titolare del trattamento non ne abbia più bisogno ai fini del trattamento, i dati personali sono necessari all'interessato per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria;
d) l'interessato si è opposto al trattamento ai sensi dell'articolo 21, paragrafo 1 RGPD, in attesa della verifica in merito all'eventuale prevalenza dei motivi legittimi del Titolare del trattamento rispetto a quelli dell'interessato.

Se il trattamento è limitato a norma del paragrafo 1 dell'art. 18 RGPD, tali dati personali sono trattati, salvo che per la conservazione, soltanto con il consenso dell'interessato o per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria oppure per tutelare i diritti di un'altra persona fisica o giuridica o per motivi di interesse pubblico rilevante dell'Unione o di uno Stato membro.
L'interessato che ha ottenuto la limitazione del trattamento a norma del paragrafo 1 è informato dal titolare prima che detta limitazione sia revocata.
Il titolare del trattamento comunica a ciascuno dei destinatari cui sono stati trasmessi i dati personali le eventuali limitazioni del trattamento salvo che ciò si riveli impossibile o implichi uno sforzo sproporzionato. Il titolare del trattamento comunica all'interessato tali destinatari qualora l'interessato lo richieda.

Art. 20
Diritto alla portabilità

Il presente Regolamento tiene conto della circostanza che, in forza della disciplina del RGPD, il diritto alla portabilità dei dati non si applica al trattamento necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento.

Art. 21
Diritto di opposizione e processo decisionale automatizzato relativo alle persone

L'interessato ha il diritto di opporsi in qualsiasi momento, per motivi connessi alla sua situazione particolare, al trattamento dei dati personali che lo riguardano ai sensi dell'articolo 6, paragrafo 1, lettere e) o f) del RGPD, compresa la profilazione sulla base di tali disposizioni.
Il titolare del trattamento si astiene dal trattare ulteriormente i dati personali salvo che egli dimostri l'esistenza di motivi legittimi cogenti per procedere al trattamento che prevalgono sugli interessi, sui diritti e sulle libertà dell'interessato oppure per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria. Il diritto di cui ai paragrafi 1 e 2 dell'art. 21 RGPD è esplicitamente portato all'attenzione dell'interessato ed è presentato chiaramente e separatamente da qualsiasi altra informazione al più tardi al momento della prima comunicazione con l'interessato.
Nel contesto dell'utilizzo di servizi della società dell'informazione e fatta salva la direttiva 2002/58/CE, l'interessato può esercitare il proprio diritto di opposizione con mezzi automatizzati che utilizzano specifiche tecniche. Qualora i dati personali siano trattati a fini di ricerca scientifica o storica o a fini statistici a norma dell'articolo 89, paragrafo 1 del RGPD, l'interessato, per motivi connessi alla sua situazione particolare, ha il diritto di opporsi al trattamento di dati personali che lo riguarda, salvo se il trattamento è necessario per l'esecuzione di un compito di interesse pubblico.

Art. 22
Modalità di esercizio dei diritti dell'interessato

Per l'esercizio dei diritti dell'interessato, in ordine all'accesso ed al trattamento dei suoi dati personali, si applicano le disposizioni del RGPD, del Codice e del presente Regolamento.
La richiesta per l'esercizio dei diritti può essere fatta pervenire:

- direttamente dall'interessato, anche facendosi assistere da una persona di fiducia, con l'esibizione di un documento personale di riconoscimento o allegandone copia o anche con altre adeguate modalità o in presenza di circostanze atte a dimostrare l'identità personale dell'interessato stesso, come ad esempio, la conoscenza personale;
- tramite altra persona fisica o associazione, a cui abbia conferito per iscritto delega o procura; in tal caso, la persona che agisce su incarico dell'interessato deve consegnare copia della procura o della delega, nonché copia fotostatica non autenticata di un documento di riconoscimento del sottoscrittore;
- tramite chi esercita la potestà o la tutela, per i minori e gli incapaci;
- in caso di persone decedute, da chi ha un interesse proprio, o agisce a tutela dell'interessato o per ragioni familiari meritevoli di protezione;
- dalla persona fisica legittimata in base ai relativi statuti od ordinamenti, se l'interessato è una persona giuridica, un ente o un'associazione.

L'interessato può presentare o inviare la richiesta di esercizio dei diritti**:**

- al titolare o Responsabile del trattamento, che conserva e gestisce i dati personali dell'interessato;
- all'ufficio protocollo generale del titolare o all'ufficio per le relazioni con il pubblico;
- Al RPD del titolare o del responsabile del trattamento, che inoltrano la richiesta agli uffici interessati.

La richiesta, per l'esercizio dei diritti di accesso ai dati personali, può essere esercitata dall'interessato solo in riferimento alle informazioni che lo riguardano e non ai dati personali relativi ai terzi, eventualmente presenti all'interno dei documenti che lo riguardano.

Fermo restando l'accesso ai dati personali, il dirigente autorizza l'esibizione degli atti all'interessato, ricorrendo le condizioni per l'accesso. I soggetti competenti alla valutazione dell'istanza sono il dirigente o un suo delegato il quale decide sull'ammissibilità della richiesta d'accesso e sulle modalità di accesso ai dati.

All'istanza deve essere dato riscontro entro 30 giorni dalla data di ricezione della stessa. I termini possono essere prolungati ad altri 30 giorni dalla data di ricezione, previa tempestiva comunicazione all'interessato, qualora l'istanza avanzata dal richiedente sia di particolare complessità o ricorra un giustificato motivo. L'accesso dell'interessato ai propri dati personali può essere differito limitatamente al periodo strettamente necessario durante il quale i dati stessi sono trattati esclusivamente per lo svolgimento di indagini difensive o per salvaguardare esigenze di riservatezza del titolare. L'accesso è tuttavia consentito agli altri dati personali dell'interessato che non incidono sulle ragioni di tutela a base del differimento.
Il titolare si conforma alle Linee guida del Garante in tema di esercizio dei diritti dell'interessato.

Art. 23
Indagini difensive

Ai fini delle indagini svolte nel corso di un procedimento penale, il difensore, ai sensi della Legge 7 dicembre 2000, n. 397 e dell'art. 391-quater del Codice di procedura penale, può chiedere documenti in possesso del titolare, e può estrarne copia, anche se contengono dati personali di un terzo interessato.
Il rilascio è subordinato alla verifica che il diritto difeso sia di rango almeno pari a quello dell'interessato, e cioè consistente in un diritto della personalità o in un altro diritto o libertà fondamentale ed inviolabile rinviando, per ogni altro e ulteriore aspetto, alla relativa disciplina al Regolamento del titolare sul diritto di accesso.
Il titolare si conforma alle Linee guida del Garante in tema di indagini difensive.

TITOLO IV
SOGGETTI

Art. 24
Titolare e contitolari

Il Titolare del Trattamento, rappresentato dal Dirigente Scolastico pro tempore, in qualità di legale rappresentante del titolare, provvede:

- a definire gli obiettivi strategici per la protezione dei dati personali in ordine al trattamento, provvedendo all'inserimento di tali obiettivi strategici nel P.T.O.F. e negli altri documenti di programmazione e pianificazione del titolare;
- a mettere in atto misure tecniche e organizzative adeguate a garantire che il trattamento sia effettuato conformemente al Codice, al RGPD e al presente Regolamento;
- a delegare ovvero a nominare, con proprio atto, le F.S. e il D.S.G.A. per i compiti, le funzioni e i poteri in ordine ai processi, procedimenti, e adempimenti relativi al trattamento dei dati personali, alla sicurezza e alla formazione, impartendo ad essi le necessarie istruzioni in relazione all'informativa agli interessati, alla tipologia dei dati da trattare, alle condizioni normative previste per il trattamento dei dati, alle modalità di raccolta, comunicazione e diffusione dei dati, all'esercizio dei diritti dell'interessato, all'adozione delle misure di sicurezza per la conservazione, protezione e sicurezza dei dati, all'eventuale uso di apparecchiature di videosorveglianza;
- a designare, con proprio atto, il Responsabile per la protezione dei dati personali; a disporre periodiche verifiche sul rispetto delle istruzioni impartite, anche con riguardo agli aspetti relativi alla sicurezza dei dati e alla formazione dei dipendenti;
- a favorire l'adesione a codici di condotta elaborati dalle associazioni e dagli organismi di categoria rappresentativi;
- a favorire l'adesione a meccanismi di certificazione;
- ad assolvere agli obblighi nei confronti del Garante nei casi previsti dalla vigente normativa;

Il titolare si trova in rapporto di contitolarità con altri titolari quando determinano congiuntamente le finalità e i mezzi del trattamento.
I contitolari sono tenuti a determinare, in modo trasparente, mediante un accordo interno, le rispettive responsabilità in merito all'osservanza degli obblighi derivanti dal RGPD e dal presente Regolamento, con particolare riguardo all'esercizio dei diritti dell'interessato, e le rispettive funzioni di comunicazione delle informazioni di cui agli articoli 13 e 14 RGPD, a meno che e nella misura in cui le rispettive responsabilità siano determinate dal diritto dell'Unione o dello Stato membro cui i titolari del trattamento sono soggetti. Tale accordo può designare un punto di contatto per gli interessati. L'accordo interno deve riflettere adeguatamente i rispettivi ruoli e i rapporti dei contitolari con gli interessati. Il contenuto essenziale dell'accordo è messo a disposizione dell'interessato.
Indipendentemente dalle disposizioni dell'accordo interno, l'interessato può esercitare i propri diritti ai sensi del presente regolamento nei confronti di e contro ciascun titolare del trattamento.

Art. 25
Funzioni Strumentali, Collaboratori del D.S. e Direttore dei Servizi Generali e Amministrativi

Il titolare conferisce alle F.S., ai C.D. e al D.S.G.A., ai sensi dell'art. 2-quaterdecies del Codice Privacy, i sottoindicati compiti e funzioni, e i correlati poteri, mediante apposito provvedimento di delega o di nomina, da adottarsi secondo il proprio ordinamento.
Nel suddetto provvedimento, il titolare deve informare ciascun F.S./C.D./D.S.G.A., delle responsabilità che gli sono affidate in relazione a quanto disposto dal Codice, dal RGPD e dal presente Regolamento. Compiti, funzioni e poteri*:*

- trattare i dati personali solo su istruzione del titolare del trattamento;

- garantire che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza;
- adottare il tempestivo ed integrale rispetto dei doveri del titolare previsti dal Codice, compreso il profilo relativo alla sicurezza del trattamento così come disciplinato nell'art. 32 del RGPD;
- osservare le disposizioni del presente Regolamento nonché delle specifiche istruzioni impartite dal titolare;
- adottare idonee misure per garantire, nell'organizzazione delle prestazioni e dei servizi, il rispetto dei diritti, delle libertà fondamentali e della dignità degli interessati, nonché del segreto professionale, fermo restando quanto previsto dalla normativa vigente, dalle disposizioni del Garante, dalle disposizioni contenute nel presente Regolamento, con particolare riguardo a tutte le disposizioni di rango speciale che comunque incidono sul trattamento dei dati;
- collaborare con il titolare del trattamento per la predisposizione del documento di valutazione d'impatto sulla protezione dei dati e per la definizione del Registro delle attività di trattamento, in collaborazione con l'amministratore di sistema e con le altre strutture competenti del titolare, nonché per gli eventuali aggiornamenti o adeguamenti del documento stesso;
- curare l'elaborazione e la raccolta della modulistica e delle informative, da utilizzarsi all'interno dell'organizzazione del titolare per l'applicazione del Codice, del RGPD, e del presente Regolamento;
- assistere il titolare del trattamento con misure tecniche ed organizzative adeguate, nella misura in cui ciò sia possibile, al fine di soddisfare l'obbligo del titolare del trattamento di dare seguito alle richieste per l'esercizio dei diritti dell'interessato per quanto previsto nella normativa vigente;
- assistere il titolare del trattamento nel garantire il rispetto degli obblighi di cui agli articoli da 32 a 36 del RGPD (sicurezza del trattamento dei dati personali, notifica di una violazione dei dati personali all'autorità di controllo, comunicazione di una violazione dei dati personali all'interessato, valutazione d'impatto sulla protezione dei dati, consultazione preventiva) tenendo conto della natura del trattamento e delle informazioni a disposizione;
- mettere a disposizione del titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi previsti nel Codice, RGPD e nel presente Regolamento;
- contribuire alle attività di verifica del rispetto del Codice, del RGPD e del presente regolamento, comprese le ispezioni, realizzate dal titolare o da un altro soggetto da questi incaricato;
- curare la costituzione e l'aggiornamento dei seguenti archivi/banche dati, per quanto di competenza:
    1. elenco dei contitolari, dei responsabili dei trattamenti, e degli incaricati, con i relativi punti di contatto;
    2. elenco degli archivi/ banche dati;
- garantire l'aggiornamento, almeno annuale, della ricognizione dei trattamenti; fornire tutte le necessarie informazioni e prestare assistenza al Responsabile della protezione dei dati (RPD/PDO) nell'esercizio delle sue funzioni.

Ciascun F.S./C.D./D.S.G.A., nell'espletamento dei compiti, funzioni e poteri delegati o per i quali ha ricevuto la nomina, collabora con il titolare al fine di:

- comunicare tempestivamente, l'inizio di ogni nuovo trattamento, la cessazione o la modifica dei trattamenti in atto, nonché ogni notizia rilevante ai fini dell'osservanza degli obblighi dettati dagli articoli da 32 a 36 del RGPD riguardanti l'adozione di misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio; la notificazione di una violazione dei dati personali al Garante privacy; la comunicazione di una violazione dei dati personali all'interessato; la redazione della valutazione d'impatto sulla protezione dei dati; la consultazione preventiva;

- somministrare le informative previste e verificarne il rispetto e la congruità con lo stato attuale dei trattamenti forniti, ed eventualmente fornire le informazioni necessarie per l'aggiornamento del registro dei trattamenti;
- attivarsi affinchè l'Istituto possa rispondere alle istanze degli interessati secondo quanto stabilito dal Codice e stabilire modalità organizzative volte a facilitare l'esercizio del diritto di accesso dell'interessato e la valutazione del bilanciamento degli interessi in gioco;
- garantire che tutte le misure di sicurezza riguardanti i dati del Titolare siano applicate all'interno della servizio/ambito di proprio riferimento ed all'esterno, qualora agli stessi vi sia accesso da parte di soggetti terzi quali responsabili del trattamento;
- informare il titolare del trattamento, senza ingiustificato ritardo, della conoscenza dell'avvenuta violazione dei dati personali.

Ciascun F.S./C.D./D.S.G.A., risponde al titolare di ogni violazione o mancata attivazione di quanto dettato dalla normativa vigente e della mancata attuazione delle misure di sicurezza.

Art. 26
Responsabili del trattamento e sub responsabili

Il Responsabile è la persona fisica o giuridica o ente pubblico che tratta i dati per conto del Titolare del trattamento. Il Responsabile è di solito un soggetto esterno ed è designato dal titolare. La designazione del responsabile del trattamento deve avvenire ogni qual volta che il titolare affida ad un soggetto esterno il trattamento di dati personali per conseguire le proprie finalità. A titolo indicativo, devono essere nominati:

- Il fornitore dei servizi di segreteria digitale
- Il fornitore dei servizi sul sito web istituzionale
- Il fornitore di servizi di assistenza e gestione dei sistemi informatici
- Consulenti e collaboratori che per lo svolgimento dell'incarico ricevuto trattano dati personali

Il Responsabile è individuato tra soggetti che per esperienza, capacità ed affidabilità forniscano idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza. Il Responsabile del trattamento non ricorre a un altro Responsabile senza previa autorizzazione scritta, specifica o generale, del titolare.
I Responsabili del trattamento hanno l'obbligo di:

- trattare i dati in modo lecito, secondo correttezza e nel pieno rispetto della normativa vigente in materia;
- rispettare le misure di sicurezza previste dal Codice sulla privacy e adottare tutte le misure che siano idonee a prevenire e/o evitare la comunicazione o diffusione dei dati, il rischio di distruzione o perdita, anche accidentale, di accesso non autorizzato o di trattamento non autorizzato o non conforme alle finalità della raccolta;
- nominare, se è il caso, al loro interno i soggetti incaricati del trattamento;
- garantire che i dati trattati siano portati a conoscenza soltanto del personale incaricato del trattamento;
- attenersi alle disposizioni impartite dal Titolare del trattamento;
- specificare i luoghi dove fisicamente avviene il trattamento dei dati e su quali supporti;
- comunicare le misure minime di sicurezza adottate per garantire la riservatezza e la protezione dei dati personali trattati.

La designazione del Responsabile viene effettuata mediante atto da parte del titolare del trattamento da allegare agli accordi, convenzioni o contratti che prevedono l'affidamento di trattamenti di dati personali esternamente al titolare. Qualora sussistano dei trattamenti di dati personali effettuati da soggetti terzi per conto del Titolare, precedenti all'adozione del presente regolamento e per i quali tali soggetti non siano stati nominati Responsabili del Trattamento secondo le indicazioni contenute

nel presente articolo, il dirigente scolastico provvede tempestivamente alla nomina degli stessi quali Responsabili del Trattamento.
L'accettazione della nomina e l'impegno a rispettare le disposizioni del Codice, del RGPD e del presente Regolamento è condizione necessaria per l'instaurarsi del rapporto giuridico fra le parti.

Art. 27
Incaricati del trattamento dipendenti del titolare

Gli incaricati del trattamento sono le persone fisiche, dipendenti del titolare, designati dal D.S., incaricati di svolgere le operazioni di trattamento dei dati personali di competenza con l'indicazione specifica dei compiti, dell'ambito di trattamento consentito, e delle modalità.
La designazione dell'incaricato al trattamento dei dati personali è di competenza del D.S.; la nomina è effettuata per iscritto e individua specificatamente i compiti spettanti all'incaricato e le modalità cui deve attenersi per l'espletamento degli stessi e l'ambito del trattamento consentito.
A prescindere dalla nomina, si considera tale anche la documentata preposizione della persona fisica ad un'unità per la quale risulti individuato, per iscritto, l'ambito del trattamento consentito agli addetti all'unità medesima. Per effetto di tale disposizione, ogni dipendente preposto ad un determinato ufficio/servizio, tenuto ad effettuare operazioni di trattamento nell'ambito di tale servizio, è da considerare, "incaricato" ai sensi dell'art. 2-quaterdecies del Codice Privacy.
Gli incaricati devono comunque ricevere idonee ed analitiche istruzioni, anche per gruppi omogenei di funzioni, riguardo le attività sui dati affidate e gli adempimenti a cui sono tenuti.
Gli incaricati collaborano con il titolare segnalando eventuali situazioni di rischio nel trattamento dei dati e fornendo ogni informazione necessaria per l'espletamento delle funzioni di controllo.
In particolare, gli incaricati devono assicurare che, nel corso del trattamento, i dati siano:

- trattati in modo lecito, corretto e trasparente nei confronti dell'interessato; raccolti e registrati per scopi determinati, espliciti e legittimi, e successivamente trattati in modo compatibile con tali finalità;
- adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati;
- esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati;
- conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore a quello necessario per il conseguimento delle finalità per le quali i dati sono trattati;
- trattati in modo tale che venga ad essere garantita un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure organizzative e tecniche adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentale.

Gli incaricati sono tenuti alla completa riservatezza sui dati di cui siano venuti a conoscenza in occasione dell'espletamento della propria attività, impegnandosi a comunicare i dati esclusivamente ai soggetti indicati dal titolare nei soli casi previsti dalla legge, nello svolgimento dell'attività istituzionale del titolare. Gli incaricati dipendenti del titolare sono destinatari degli interventi di formazione di aggiornamento.

Art. 28
Incaricati del trattamento non dipendenti del titolare

Tutti i soggetti che svolgono un'attività di trattamento dei dati, e che non sono dipendenti del titolare, quali a titolo meramente esemplificativo i tirocinanti, i volontari e i soggetti che operano temporaneamente all'interno della struttura organizzativa del titolare o incaricati nominati dal Responsabile esterno, devono essere incaricati del trattamento tramite atto scritto di nomina.

Questi ultimi sono soggetti agli stessi obblighi cui sono sottoposti tutti gli incaricati dipendenti del titolare, in modo da garantire il pieno rispetto della tutela della riservatezza dei dati.
Gli incaricati non dipendenti dal titolare sono destinatari degli interventi di formazione di aggiornamento.

Art. 29

Responsabile della protezione dei dati personali (RPD) - Data Protection Officer (DPO)

Il Titolare designa il Responsabile della protezione dei dati (RPD/DPO). Il RPD/PDO deve essere in possesso di:

- un'adeguata conoscenza della normativa e delle prassi di gestione dei dati personali;
- deve adempiere alle sue funzioni in totale indipendenza e in assenza di conflitti di interesse;
- operare alle dipendenze del titolare del trattamento oppure sulla base di un contratto di servizio.

Il RPD/DPO è tenuto al segreto o alla riservatezza in merito all'adempimento dei propri compiti.
Il titolare del trattamento mette a disposizione del DPO le risorse necessarie per adempiere ai suoi compiti e accedere ai dati personali e ai trattamenti. Il RPD/PDO svolge i seguenti compiti:

- informa e fornisce consulenze al titolare del trattamento, nonché ai dipendenti che eseguono il trattamento dei dati in merito agli obblighi vigenti relativi alla protezione dei dati;
- verifica l'attuazione e l'applicazione della normativa vigente in materia, nonché delle politiche del Titolare o del Responsabile del trattamento relative alla protezione dei dati personali, inclusi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale coinvolto nelle operazioni di trattamento, e gli audit relativi;
- fornisce, qualora venga richiesto, pareri in merito alla valutazione d'impatto sulla protezione dei dati e sorveglia i relativi adempimenti;
- funge da punto di contatto per gli interessati in merito al trattamento dei loro dati personali e all'esercizio dei diritti;
- funge da punto di contatto con il Garante per la protezione dei dati personali per questioni connesse al trattamento dei dati, tra cui la consultazione preventiva.

TITOLO V

SICUREZZA DEI DATI PERSONALI

Art. 30

Misure di sicurezza

Il titolare, nel trattamento dei dati personali, garantisce l'applicazione di adeguate e misure di sicurezza che consentono di ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alla finalità della raccolta.
In particolare il titolare del trattamento mette in atto misure e tecniche, organizzative, di gestione, procedurali e documentali adeguate a garantire un livello di sicurezza adeguato al rischio. Tali misure possono comprendere :

- la pseudonimizzazione e la cifratura dei dati personali trattati;
- procedure per assicurare, in modo permanente, la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
- modalità per garantire il ripristino tempestivo nell'accesso ai dati personali in caso di incidente fisico o tecnico;
- una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

Art. 31

Valutazione d'impatto sulla protezione dei dati - DPIA

La valutazione d'impatto sulla protezione dei dati (di seguito solo "DPIA") è un processo inteso a descrivere il trattamento, valutarne la necessità e la proporzionalità, nonché a contribuire a gestire i rischi per i diritti e le libertà delle persone fisiche derivanti dal trattamento di dati personali, valutando detti rischi e determinando le misure per affrontarli.

La DPIA è uno strumento importante per la responsabilizzazione in quanto sostiene il titolare non soltanto nel rispettare i requisiti del RGPD, ma anche nel dimostrare che sono state adottate misure appropriate per garantire il rispetto del medesimo RGPD. La DPIA sulla protezione dei dati personali deve essere realizzata, prima di procedere al trattamento, dal titolare del trattamento quando un tipo di trattamento, considerata la natura, il contesto, le finalità, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche. Qui si intende per "rischio" uno scenario che descrive un evento e le sue conseguenze, stimato in termini di gravità e probabilità, e per "gestione dei rischi" l'insieme delle attività coordinate volte a indirizzare e controllare un'organizzazione in relazione ai rischi. Prioritariamente alla DPIA deve:

- essere effettuata o aggiornata la ricognizione dei trattamenti.
- essere effettuata la determinazione in ordine alla possibilità che il trattamento possa determinare un rischio elevato per i diritti e le libertà degli interessati.

La decisione in ordine alla possibilità che il trattamento possa produrre un rischio elevato sulla protezione dei dati delle persone fisiche e, quindi, sulla obbligatorietà della DPIA viene adottata applicando i casi indicati all'art. 35, paragrafo 3 del RGPD ed i criteri esplicativi contenuti nelle ***"Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento possa presentare un rischio elevato ai fini del regolamento (UE) 2016/679"*** adottate dal Garante il 4 aprile 2017 e tenendo conto di eventuali successive modifiche (di seguito solo "Linee guida").

Nell'applicare i suddetti criteri si deve tenere conto di quanto segue:

- la DPIA è sempre obbligatoria, indipendentemente dalla presenza di uno o più criteri sopra menzionati, per tutti i trattamenti inclusi nell'elenco predisposto e pubblicato dall'Autorità di controllo ai sensi dell'art. 35, paragrafo 4 RGPD;
- fermo restando che, secondo le Linee guida, un trattamento che soddisfa 2 criteri deve formare oggetto di una valutazione d'impatto sulla protezione dei dati, tuttavia, al fine di garantire una maggiore garanzia di tutela, la ricorrenza anche di 1 solo criterio potrebbe costituire elemento sufficiente per originare l'obbligo di svolgimento della DPIA;
- maggiore è il numero di criteri soddisfatti dal trattamento, più è probabile che sia presente un rischio elevato per i diritti e le libertà degli interessati e, di conseguenza, che sia necessario realizzare una valutazione d'impatto sulla protezione dei dati;

La DPIA non è richiesta nei seguenti casi:

- quando, sulla base di predetti criteri, risulta che il trattamento non è tale da "presentare un rischio elevato per i diritti e le libertà delle persone fisiche";
- quando la natura, l'ambito di applicazione, il contesto e le finalità del trattamento sono molto simili a un trattamento per il quale è stata svolta una valutazione d'impatto sulla protezione dei dati. In tali casi, si possono utilizzare i risultati della valutazione d'impatto sulla protezione dei dati per un trattamento analogo;
- quando le tipologie di trattamento sono state verificate da un'autorità di controllo prima del maggio 2018 in condizioni specifiche che non sono cambiate;
- qualora un trattamento, effettuato a norma dell'articolo 6, paragrafo 1, lettere c) o e) GPDR, trovi una base giuridica nel diritto dell'Unione o nel diritto dello Stato membro, tale diritto

disciplini il trattamento specifico o sia già stata effettuata una valutazione d'impatto sulla protezione dei dati nel contesto dell'adozione di tale base giuridica (articolo 35, paragrafo 10 GPDR).

Secondo quanto disposto dall'art. 35, paragrafo 7 del RGPD, la DPIA deve contenere almeno:

- una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal Titolare del trattamento;
- una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità;
- una valutazione dei rischi per i diritti e le libertà degli interessati;
- le misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione. Quando insorgono variazioni del rischio rappresentato dalle attività relative al trattamento, il titolare del trattamento, se necessario, procede a un riesame della valutazione d'impatto sulla protezione dei dati.

Laddove la DPIA riveli la presenza di rischi residui elevati, il titolare è tenuto a richiedere la consultazione preventiva dell'autorità di controllo in relazione al trattamento ai sensi dell'art. 36, paragrafo 1 RGPD.

Art. 32
Pubblicazione sintesi della valutazione d'impatto - DPIA

Il titolare, previa analisi interna sulle potenziali ricadute, effettua la pubblicazione della DPIA o di una sintesi della stessa al fine di contribuire a stimolare la fiducia nei confronti dei trattamenti effettuati dal titolare, nonché di dimostrare la responsabilizzazione e la trasparenza.
La DPIA pubblicata non deve contenere l'intera valutazione qualora essa possa presentare informazioni specifiche relative ai rischi per la sicurezza per il titolare o divulgare segreti commerciali o informazioni commerciali sensibili. In queste circostanze, la versione pubblicata potrebbe consistere soltanto in una sintesi delle principali risultanze della DPIA o addirittura soltanto in una dichiarazione nella quale si afferma che la DPIA è stata condotta.

Art. 33
Consultazione preventiva

1. Nei casi in cui si è proceduto nella valutazione di impatto sulla protezione dei dati ed è emerso che l'Istituto non riesce a trattare in maniera sufficiente tutti i rischi elevati, poiché ne restano ancora alcuni per questi ultimi residui, va consultato preventivamente il Garante per la privacy.
2. L'Istituto, tramite il Responsabile della protezione dei dati ai sensi degli artt. 36 e 39, par. 1, lett. e), Regolamento UE n. 679/2016, invia richiesta di consultazione al Garante comunicando:
    a. i dati dell'Istituto in quanto Titolare del trattamento ed i propri dati in quanto punto di contatto e referente per la consultazione;
    b. le finalità ed i mezzi di trattamento previsti;
    c. le misure di garanzia previste per proteggere i diritti e le libertà fondamentali degli interessati;
    d. la valutazione di impatto sulla protezione dei dati in versione completa; – ogni altra informazione ritenuta necessaria.
3. Il Garante formula parere scritto entro otto settimane dal ricevimento della richiesta di consultazione nel caso in cui ritenga che il trattamento comunicato violi le norme sulla protezione dei dati ed in particolare qualora ritenga che il Titolare non abbia sufficientemente

attenuato o identificato il rischio. In base alla complessità del trattamento previsto il Garante può prorogare la sua risposta di un termine aggiuntivo di sei settimane informando il Responsabile della protezione dei dati, entro un mese dal ricevimento della richiesta di consultazione.

4. In caso sia necessario, il Garante può richiedere al Responsabile della protezione dei dati informazioni aggiuntive a quelle già comunicate e può sospendere la decorrenza dei termini di cui al comma 3 in attesa della loro trasmissione.
5. In assenza di parere espresso del Garante entro le otto settimane dal ricevimento della richiesta di consultazione, l'Istituto può procedere nel trattamento dei dati.

Art. 34

Modulistica e procedure

Il titolare, al fine di agevolare e semplificare la corretta e puntuale applicazione delle disposizioni del Codice, del RGPD, del presente Regolamento, e di tutte le linee guida e provvedimenti del Garante:

a) adotta e costantemente aggiorna:
   - modelli uniformi di informativa;
   - modelli e formule uniformi necessarie per gestire il trattamento dei dati e le misure di sicurezza;
b) elabora, approva, e costantemente aggiorna:
   - adeguate procedure gestionali, da raccogliere in un apposito Manuale delle procedure.

Art. 35

Responsabilità in caso di violazione delle disposizioni in materia di protezione dei dati personali

Il mancato rispetto delle disposizioni in materia di riservatezza dei dati personali è sanzionato come previsto dagli articoli da 161 a 172 del Codice da parte del Garante, nonché con sanzioni di natura disciplinare.

Il Titolare del trattamento risponde per il danno cagionato dal suo trattamento che violi il presente regolamento.

Il Responsabile del trattamento risponde per il danno causato dal trattamento solo se non ha adempiuto agli obblighi previsti nel Codice nel RGPD e nel presente regolamento, e a lui specificamente diretti o ha agito in modo difforme o contrario rispetto alle legittime istruzioni impartitegli dal titolare del trattamento.

Art. 36

Violazione dei dati personali

L'Istituto redige uno specifico regolamento per la definizione delle modalità di individuazione, gestione e notifica di violazioni dei dati personali (*Data breach*). Tale regolamento contiene le informazioni riguardanti le procedure da seguire in caso di sospetto di avvenuta violazione. Destinatari dello stesso sono tutti i delegati e gli incaricati al trattamento dati personali all'interno dell'amministrazione.

TITOLO VII

ENTRATA IN VIGORE E DISPOSIZIONI FINALI

Art. 37

Entrata in vigore del regolamento

1. Il presente regolamento entra in vigore il giorno in cui diviene esecutiva la relativa Determina del Dirigente.

2. Il regolamento e la relativa modulistica per l'esercizio dei diritti sono resi pubblici mediante pubblicazione sul sito internet dell'Istituto, nella Sezione Amministrazione Trasparente.
3. Copia del regolamento va inoltrata alle Funzioni Strumentali ed ai responsabili di servizio, al RPD, ai Responsabili del trattamento, ai sub-responsabili ed ogni altro dipendente che tratta dati personali nell'Istituto. In alternativa, può essere data agli stessi comunicazione della disponibilità online del presente regolamento, contenente le coordinate web a quale esso è accessibile, tramite una comunicazione effettuata tramite i canali ufficiali dell'Istituto.

Art. 38
Disposizioni finali

Per quanto non previsto nel presente Regolamento si applicano le disposizioni del Codice, del RGPD, le Linee guida e i provvedimenti del Garante.
Il presente Regolamento è aggiornato a seguito di ulteriori modificazioni alla vigente normativa in materia di riservatezza e protezione dei dati personali.
Il testo del presente Regolamento potrà essere aggiornato con atto deliberativo del Dirigente Scolastico, su indicazioni del DPO, a seguito di eventuali modifiche che intervengano rispetto alla vigente normativa, sia nazionale che regionale, in materia di protezione dei dati personali.
Gli eventuali aggiornamenti ai documenti allegati verranno, pertanto, inseriti in tempo reale sul sito internet nell'apposita sezione dedicata alla "privacy", prescindendo dall'adozione di appositi atti deliberativi di modifica del presente Regolamento e dandone pubblicità per mezzo di circolari indirizzate a tutti i possibili interessati, così da consentire una rapida consultazione on line dei medesimi ed un contenuto sempre aggiornato degli stessi.

Quartu Sant'Elena, 03/04/24

Il Dirigente Scolastico
Prof. Massimo Mocci

Documento informatico firmato digitalmente ai sensi del D.Lgs 82/2005 s.m.i. e norme collegate, il quale sostituisce il documento cartaceo e la firma autografa

Liceo Classico Linguistico e Scienze Umane B.R. Motzo

Sede: Via Don Sturzo, 4, 09045 Quartu Sant'Elena (CA)

Telefono: 070/825629 **Sito istituzionale:** liceomotzo.edu.it

E-mail: CAPC09000E@istruzione.it **PEC:** CAPC09000E@pec.istruzione.it

C.U.: UFAGLG **C.F.:** 92168540927

ALLEGATO I: REGOLAMENTO DI ISTITUTO PER LA GESTIONE DELLE VIOLAZIONI DEI DATI PERSONALI

Il Regolamento Generale sulla Protezione dei Dati (Reg. UE 679/2016), di seguito il Regolamento, introduce l'obbligo di notificare una violazione dei dati personali (in appresso: "violazione") all'autorità di controllo nazionale competente (oppure, in caso di violazione transfrontaliera, all'autorità capofila) e, in alcuni casi, di comunicare la violazione alle singole persone fisiche i cui dati personali sono stati interessati dalla violazione.

Una violazione dei dati personali può, se non affrontata in modo adeguato e tempestivo, provocare danni fisici, materiali o immateriali alle persone fisiche, ad esempio perdita del controllo dei dati personali che li riguardano o limitazione dei loro diritti, discriminazione, furto o usurpazione d'identità, perdite finanziarie, decifratura non autorizzata della pseudonimizzazione, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale o qualsiasi altro danno economico o sociale significativo alla persona fisica interessata.

Pertanto, non appena viene a conoscenza di un'avvenuta violazione dei dati personali, il titolare del trattamento dovrebbe notificare la violazione dei dati personali all'autorità di controllo competente, senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che il titolare del trattamento non sia in grado di dimostrare che, conformemente al principio di responsabilizzazione, è improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Oltre il termine di 72 ore, tale notifica dovrebbe essere corredata delle ragioni del ritardo e le informazioni potrebbero essere fornite in fasi successive senza ulteriore ingiustificato ritardo.

Al fine di identificare e, se necessario, notificare correttamente un data breach all'autorità garante competente e/o agli interessati, il Dirigente Scolastico intende definire le procedure da seguire qualora avvenga un presunto data breach all'interno dell'amministrazione. Si ricorda che la mancata notifica, qualora sia essa necessaria, può comportare una sanzione amministrativa fino ad un importo di 10 milioni di euro oppure il 2% del fatturato dell'intera società.

Il presente regolamento di istituto è stato redatto sulla base delle Linee guida sulla notifica delle violazioni dei dati personali ai sensi del regolamento (UE) 2016/679, redatto dal gruppo di lavoro articolo 29 per la protezione dei dati, adottate il 3 ottobre 2017 e nella versione emendata e adottata in data 6 febbraio 2018.

Tali linee guida sono reperibili sul sito del garante per la protezione dei dati personali al link https://www.garanteprivacy.it/regolamentoue/databreach.

Sommario

ARTICOLO 1: DEFINIZIONE DI VIOLAZIONE

Per poter porre rimedio a una violazione occorre innanzitutto che il titolare del trattamento sia in grado di riconoscerla. All'articolo 4, punto 12, il regolamento definisce la "violazione dei dati personali" come segue:

> "la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati".

Di seguito una descrizione della terminologia, come descritto dal Garante per la Protezione dei Dati personali:

- **Distruzione:** il significato di "distruzione" dei dati personali dovrebbe essere abbastanza chiaro: si ha distruzione dei dati quando gli stessi non esistono più o non esistono più in una forma che sia di qualche utilità per il titolare del trattamento.
- **Perdita:** Con "perdita" dei dati personali si dovrebbe invece intendere il caso in cui i dati potrebbero comunque esistere, ma il titolare del trattamento potrebbe averne perso il controllo o l'accesso, oppure non averli più in possesso.
- **Divulgazione o accesso:** un trattamento non autorizzato o illecito può includere la divulgazione di dati personali a (o l'accesso da parte di) destinatari non autorizzati a ricevere (o ad accedere a) i dati oppure qualsiasi altra forma di trattamento in violazione del regolamento.
- **Modifica:** si verifica un danno quando i dati personali sono stati modificati, corrotti o non sono più completi.

Un esempio di perdita di dati personali può essere la perdita o il furto di un dispositivo contenente una copia della banca dati dei clienti del titolare del trattamento. Un altro esempio può essere il caso in cui l'unica copia di un insieme di dati personali sia stata crittografata da un *ransomware* (*malware* del riscatto) oppure dal titolare del trattamento mediante una chiave non più in suo possesso. Ulteriori esempi possono essere visionati nell'allegato B al presente regolamento.

Inoltre, le violazioni possono essere classificate in base ai seguenti tre principi ben noti della sicurezza delle informazioni:
• "violazione della riservatezza", in caso di divulgazione dei dati personali o accesso agli stessi non autorizzati o accidentali;
• "violazione dell'integrità", in caso di modifica non autorizzata o accidentale dei dati personali;
• "violazione della disponibilità", in caso di perdita, accesso o distruzione accidentali o non autorizzati di dati personali.

Va altresì osservato che, a seconda dei casi, una violazione può riguardare contemporaneamente la riservatezza, l'integrità e la disponibilità dei dati personali, nonché qualsiasi combinazione delle stesse.

Esempi di perdita di disponibilità possono aversi quando i dati vengono cancellati accidentalmente o da una persona non autorizzata, oppure, in caso di dati crittografati in maniera sicura, quando la chiave di decifratura viene persa. Se il titolare del trattamento non è in grado di ripristinare l'accesso ai dati, ad esempio ricorrendo a un backup, la perdita di disponibilità sarà considerata permanente.

Può verificarsi perdita di disponibilità anche in caso di interruzione significativa del servizio abituale di un'organizzazione, ad esempio un'interruzione di corrente o attacco da "blocco di servizio" (*denial of service*) che rende i dati personali indisponibili.

ARTICOLO 2: QUANDO È NECESSARIO NOTIFICARE LA VIOLAZIONE AL GARANTE O AGLI INTERESSATI? QUALI SONO LE TEMPISTICHE DI NOTIFICA?

Il regolamento impone al **titolare del trattamento** di notificare le violazioni all'autorità di controllo competente, fatta salva l'improbabilità che la violazione presenti il rischio che si verifichino detti effetti negativi. Laddove sia altamente probabile che tali effetti negativi si verifichino, il regolamento impone al titolare del trattamento di comunicare la violazione alle persone fisiche interessate non appena ciò sia ragionevolmente fattibile.

Più nel dettaglio, l'Art. 33, paragrafo 1 del regolamento impone che: In caso di violazione dei dati personali, il titolare del trattamento notifica la violazione all'autorità di controllo competente (…) senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, **a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche**. Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, è corredata dei motivi del ritardo.

Il Garante privacy ha pubblicato sul proprio sito istituzionale un importante strumento di autovalutazione che consiglia le azioni da intraprendere in seguito di un'avvenuta violazione di dati personali e reperibile al sito https://servizi.gpdp.it/databreach/s/self-assessment

Il momento esatto in cui il titolare del trattamento può considerarsi "a conoscenza" di una particolare violazione dipenderà dalle circostanze della violazione. In alcuni casi sarà relativamente evidente fin dall'inizio che c'è stata una violazione, mentre in altri potrebbe occorrere del tempo per stabilire se i dati personali sono stati compromessi. Tuttavia, l'accento dovrebbe essere posto sulla tempestività dell'azione per indagare su un incidente per stabilire se i dati personali sono stati effettivamente violati e, in caso affermativo, prendere misure correttive ed effettuare la notifica, se necessario.

L'autorità garante riporta alcuni esempi a riguardo:

1. In caso di perdita di una chiave USB contenente dati personali non crittografati spesso non è possibile accertare se persone non autorizzate abbiano avuto accesso ai dati. Tuttavia, anche se il titolare del trattamento non è in grado di stabilire se si è verificata una violazione della riservatezza, tale caso deve essere notificato, in quanto sussiste una ragionevole certezza del fatto che si è verificata una violazione della disponibilità; il titolare del trattamento si considera venuto "a conoscenza" della violazione nel momento in cui si è accorto di aver perso la chiave USB.
2. Un terzo informa il titolare del trattamento di aver ricevuto accidentalmente i dati personali di uno dei suoi clienti e fornisce la prova della divulgazione non autorizzata. Dato che al titolare del trattamento è stata presentata una prova evidente di una violazione della riservatezza, non vi è dubbio che ne sia venuto "a conoscenza".
3. Un titolare del trattamento rileva che c'è stata una possibile intrusione nella sua rete. Controlla quindi i propri sistemi per stabilire se i dati personali ivi presenti sono stati compromessi e ne ottiene conferma. Ancora una volta, dato che il titolare del trattamento ha una chiara prova di una violazione non può esserci dubbio che sia venuto "a conoscenza" della stessa.
4. Un criminale informatico viola il sistema del titolare del trattamento e lo contatta per chiedere un riscatto. In tal caso, dopo aver verificato il suo sistema per accertarsi dell'attacco, il titolare

del trattamento dispone di prove evidenti che si è verificata una violazione e non vi è dubbio che ne sia venuto a conoscenza.

5. Una persona informa il titolare del trattamento di aver ricevuto un'e-mail da un soggetto che si fa passare per il titolare del trattamento, contenente dati personali relativi al suo (effettivo) utilizzo del servizio del titolare del trattamento, aspetto questo che suggerisce che la sicurezza del titolare del trattamento sia stata compromessa. Il titolare del trattamento conduce una breve indagine e individua un'intrusione nella propria rete e la prova di un accesso non autorizzato ai dati personali. Il titolare del trattamento si considera "a conoscenza" della violazione in questo momento e dovrà procedere alla notifica all'autorità di controllo a meno che sia improbabile che la violazione presenti un rischio per i diritti e le libertà delle persone fisiche. Il titolare del trattamento dovrà prendere le opportune misure correttive per far fronte alla violazione.

Di conseguenza, il titolare del trattamento dovrebbe disporre di procedure interne per poter rilevare una violazione e porvi rimedio. Ad esempio, per rilevare talune irregolarità nel trattamento dei dati, il titolare o il responsabile del trattamento può utilizzare alcune misure tecniche certe come il flusso di dati e gli analizzatori di registri, dai quali è possibile definire eventi e allerte correlando qualsiasi dato di registro. È importante che quando viene rilevata una violazione, la stessa venga segnalata al livello superiore appropriato di gestione, in maniera da poter essere trattata e, se del caso, notificata in conformità all'articolo 33 e, se necessario, all'articolo 34.

ARTICOLO 3: PROCEDURE DA ADOTTARE IN CASO DI PRESUNTA VIOLAZIONE DEI DATI PERSONALI

Qualora un dipendente dell'amministrazione rilevi una possibile violazione dei dati personali (vedasi allegato B per una lista di esempio degli stessi), esso è tenuto ad informarne il Dirigente Scolastico o, qualora esso non sia immediatamente disponibile, il Responsabile della Protezione dei Dati (tramite l'indirizzo mail ordinario dpo@mariomuredduconsulting.com), indicando i propri dati di contatto.

A questo punto il D.S., in concerto con l'RPD e l'amministratore di sistema informatico (qualora si tratti di una violazione informatica), provvederà ad effettuare una prima indagine interna e a definire la gravità dell'eventuale violazione. In particolare, si dovrà procedere a identificare i possibili rischi da essa derivanti e a definire le ulteriori azioni da intraprendere.

ARTICOLO 4: MODALITÀ DI NOTIFICA AL GARANTE E AGLI INTERESSATI

Quando il titolare del trattamento notifica una violazione all'autorità di controllo, l'articolo 33, paragrafo 3 stabilisce che la notifica deve almeno:

"a) descrivere la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;

comunicare il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;

descrivere le probabili conseguenze della violazione dei dati personali;

descrivere le misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi".

A tal fine, l'autorità Garante per la Protezione dei Dati Personali ha messo a disposizione un modello di segnalazione dei data breach, disponibile al link: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1915835.

Il regolamento non definisce le categorie di interessati né le registrazioni di dati personali. Tuttavia, il Gruppo di lavoro suggerisce che le categorie di interessati si riferiscono ai vari tipi di persone fisiche i cui dati personali sono stati oggetto di violazione: a seconda dei descrittori utilizzati, ciò potrebbe includere, tra gli altri, minori e altri gruppi vulnerabili, persone con disabilità, dipendenti o clienti.

Analogamente, le categorie di registrazioni dei dati personali fanno riferimento ai diversi tipi di registrazioni che il titolare del trattamento può trattare, quali dati sanitari, registri didattici, informazioni sull'assistenza sociale, dettagli finanziari, numeri di conti bancari, numeri di passaporto, ecc.

Il considerando 85 chiarisce che uno degli scopi della notifica consiste nel limitare i danni alle persone fisiche. Di conseguenza, se i tipi di interessati o di dati personali rivelano un rischio di danno particolare a seguito di una violazione (ad esempio usurpazione d'identità, frode, perdite finanziarie, minaccia al segreto professionale) è importante che la notifica indichi tali categorie. In questo modo, l'obbligo di descrivere le categorie si collega all'obbligo di descriverne le probabili conseguenze della violazione.

Il fatto che non siano disponibili informazioni precise (ad esempio il numero esatto di interessati coinvolti) non dovrebbe costituire un ostacolo alla notifica tempestiva delle violazioni. Il regolamento consente di effettuare approssimazioni sul numero di persone fisiche interessate e di registrazioni dei dati personali coinvolte. Ci si dovrebbe preoccupare di far fronte agli effetti negativi della violazione piuttosto che di fornire cifre esatte. Di conseguenza, quando è evidente che c'è stata una violazione ma non se ne conosce ancora la portata, un modo sicuro per soddisfare gli obblighi di notifica è procedere a una notifica per fasi (cfr. in appresso).

L'articolo 33, paragrafo 3, stabilisce che nella notifica il titolare del trattamento "deve almeno" fornire le informazioni previste; di conseguenza il titolare del trattamento può, se necessario, fornire ulteriori informazioni. I diversi tipi di violazioni (riservatezza, integrità o disponibilità) possono richiedere la fornitura di ulteriori informazioni per spiegare in maniera esaustiva le circostanze di ciascun caso.

Esempio

Nell'ambito della notifica all'autorità di controllo, il titolare del trattamento può ritenere utile indicare il nome del responsabile del trattamento, qualora quest'ultimo sia la causa di fondo della violazione, in particolare se quest'ultima ha provocato un incidente ai danni delle registrazioni dei dati personali di molti altri titolari del trattamento che fanno ricorso al medesimo responsabile del trattamento.

In ogni caso, l'autorità di controllo può richiedere ulteriori dettagli nel contesto dell'indagine su una violazione.

Notifica per fasi

A seconda della natura della violazione, il titolare del trattamento può avere la necessità di effettuare ulteriori accertamenti per stabilire tutti i fatti pertinenti relativi all'incidente. L'articolo 33, paragrafo 4, afferma pertanto:

> "Qualora e nella misura in cui non sia possibile fornire le informazioni contestualmente, le informazioni possono essere fornite in fasi successive senza ulteriore ingiustificato ritardo".

Ciò significa che il regolamento prende atto del fatto che il titolare del trattamento non sempre dispone di tutte le informazioni necessarie su una violazione entro 72 ore dal momento in cui ne è venuto a conoscenza, dato che non sempre sono disponibili entro tale termine dettagli completi ed esaustivi su un incidente. Pertanto, il regolamento consente una notifica per fasi. È più probabile che ciò si verifichi in caso di violazioni più complesse, quali alcuni tipi di incidenti di sicurezza informatica nel contesto dei quali, ad esempio, può essere necessaria un'indagine forense approfondita per stabilire appieno la natura della violazione e la portata della compromissione dei dati personali. Di conseguenza, in molti casi il titolare del trattamento dovrà effettuare ulteriori indagini e dare seguito alla notifica fornendo informazioni supplementari in un secondo momento. Ciò è consentito a condizione che il titolare del trattamento indichi i motivi del ritardo, in conformità all'articolo 33, paragrafo 1. Il Gruppo di lavoro raccomanda che, all'atto della prima notifica all'autorità di controllo, il titolare del trattamento informi quest'ultima del fatto che non dispone ancora di tutte le informazioni richieste e che fornirà ulteriori dettagli in un momento successivo. L'autorità di controllo dovrebbe concordare le modalità e le tempistiche per la fornitura delle informazioni supplementari. Questo non impedisce al titolare del trattamento di trasmettere ulteriori informazioni in qualsiasi altro momento, qualora venga a conoscenza di ulteriori dettagli rilevanti sulla violazione che devono essere forniti all'autorità di controllo.

L'obiettivo dell'obbligo di notifica consiste nell'incoraggiare il titolare del trattamento ad agire prontamente in caso di violazione, a contenerla e, se possibile, a recuperare i dati personali compromessi e a chiedere un parere pertinente all'autorità di controllo. La notifica all'autorità di controllo entro le prime 72 ore può consentire al titolare del trattamento di assicurarsi che le decisioni in merito alla notifica o alla mancata notifica alle persone fisiche siano corrette.

Tuttavia, lo scopo della notifica all'autorità di controllo non è solo di ottenere orientamenti sull'opportunità di effettuare o meno la notifica alle persone fisiche interessate. In certi casi sarà evidente che, a causa della natura della violazione e della gravità del rischio, il titolare del trattamento dovrà effettuare la notifica alle persone fisiche coinvolte senza indugio. Ad esempio, se esiste una minaccia immediata di usurpazione d'identità oppure se categorie particolari di dati personali vengono divulgate online, il titolare del trattamento deve agire senza ingiustificato ritardo per contenere la violazione e comunicarla alle persone fisiche coinvolte (cfr. sezione III). In circostanze eccezionali, ciò potrebbe persino aver luogo prima della notifica all'autorità di controllo. Più in generale, la notifica all'autorità di controllo non può fungere da giustificazione per la mancata comunicazione della violazione all'interessato laddove la comunicazione sia richiesta.

È opportuno inoltre precisare che se, dopo la notifica iniziale, una successiva indagine dimostra che l'incidente di sicurezza è stato contenuto e che non si è verificata alcuna violazione il titolare del trattamento può informarne l'autorità di controllo. Tali informazioni possono quindi essere aggiunte alle informazioni già fornite all'autorità di controllo e l'incidente può essere quindi registrato come un evento che non costituisce una violazione. Non si incorre in alcuna sanzione se si segnala un incidente che alla fine si rivela non essere una violazione.

Esempio

Un titolare del trattamento notifica all'autorità di controllo entro 72 ore l'individuazione di una violazione derivante dalla perdita di una chiave USB contenente una copia dei dati personali di alcuni dei suoi clienti. In seguito scopre che la chiave USB non era stata messa al suo posto e la recupera. Il titolare del trattamento aggiorna l'autorità di controllo e chiede la modifica della notifica.

Va osservato che un approccio per fasi alla notifica esiste già in forza degli obblighi di cui alla direttiva 2002/58/CE, del regolamento 611/2013 e nel quadro di altri incidenti segnalati di propria iniziativa.

Notifiche effettuate in ritardo

L'articolo 33, paragrafo 1, chiarisce che, qualora non sia effettuata entro 72 ore, la notifica all'autorità di controllo deve essere corredata dei motivi del ritardo. Questa disposizione, unitamente al concetto di notifica in fasi, riconosce che il titolare del trattamento potrebbe non essere sempre in grado di notificare una violazione entro tale termine e che una notifica tardiva può essere consentita.

Tale scenario potrebbe aver luogo, ad esempio, qualora il titolare del trattamento subisca in poco tempo violazioni della riservatezza multiple e simili che coinvolgono allo stesso modo un gran numero di interessati. Il titolare del trattamento potrebbe prendere atto di una violazione e, nel momento in cui inizia l'indagine e prima della notifica, rilevare ulteriori violazioni analoghe, che hanno cause differenti. A seconda delle circostanze, il titolare del trattamento può impiegare del tempo per stabilire l'entità delle violazioni e, anziché notificare ciascuna violazione separatamente, effettuare una notifica significativa che rappresenta diverse violazioni molto simili tra loro, con possibili cause diverse. La notifica all'autorità di controllo potrebbe quindi aver luogo in ritardo, oltre le 72 ore dopo che il titolare del trattamento è venuto a conoscenza di tali violazioni.

A rigore di termini, ogni singola violazione costituisce un incidente segnalabile. Tuttavia, per evitare che il processo diventi eccessivamente oneroso, il titolare del trattamento può presentare una notifica "cumulativa" che rappresenta tutte le violazioni in questione, a condizione che riguardino il medesimo tipo di dati personali e che questi siano stati violati nel medesimo modo in un lasso di tempo relativamente breve. Se si verificano diverse violazioni riguardanti tipi diversi di dati personali, violati in maniere diverse, la notifica deve procedere secondo l'iter normale, segnalando ogni violazione conformemente all'articolo 33.

Sebbene il regolamento consenta di effettuare la notifica in ritardo, questa non dovrebbe essere vista come la regola. È opportuno sottolineare che le notifiche cumulative possono essere effettuate anche per più violazioni analoghe segnalate entro 72 ore.

Notifiche agli interessati

In alcuni casi, oltre a effettuare la notifica all'autorità di controllo, il titolare del trattamento è tenuto a comunicare la violazione alle persone fisiche interessate.

L'articolo 34, paragrafo 1, afferma che:

"Quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento comunica la violazione all'interessato senza ingiustificato ritardo".

Il titolare del trattamento dovrebbe tenere a mente che la notifica all'autorità di controllo è obbligatoria a meno che sia improbabile che dalla violazione possano derivare rischi per i diritti e le libertà delle persone

fisiche. Inoltre, laddove la violazione presenti un rischio elevato per i diritti e le libertà delle persone fisiche occorre informare anche queste ultime. La soglia per la comunicazione delle violazioni alle persone fisiche è quindi più elevata rispetto a quella della notifica alle autorità di controllo, pertanto non tutte le violazioni dovranno essere comunicate agli interessati, il che li protegge da inutili disturbi arrecati dalla notifica.

Il regolamento afferma che la comunicazione di una violazione agli interessati dovrebbe avvenire "senza ingiustificato ritardo", il che significa il prima possibile. L'obiettivo principale della comunicazione agli interessati consiste nel fornire loro informazioni specifiche sulle misure che questi possono prendere per proteggersi. Come osservato in precedenza, a seconda della natura della violazione e del rischio presentato, la comunicazione tempestiva aiuterà le persone a prendere provvedimenti per proteggersi da eventuali conseguenze negative della violazione.

L'allegato B delle presenti linee guida fornisce un elenco non esaustivo di esempi di casi in cui una violazione può presentare un rischio elevato per le persone fisiche e, di conseguenza, in cui il titolare del trattamento deve comunicarla agli interessati.

Informazioni da fornire nelle notifiche agli interessati

Ai fini della comunicazione alle persone fisiche, l'articolo 34, paragrafo 2, specifica che:

> "La comunicazione all'interessato di cui al paragrafo 1 del presente articolo descrive con un linguaggio semplice e chiaro la natura della violazione dei dati personali e contiene almeno le informazioni e le misure di cui all'articolo 33, paragrafo 3, lettere b), c) e d)".

Secondo tale disposizione, il titolare del trattamento deve fornire almeno le seguenti informazioni:

- una descrizione della natura della violazione;
- il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto;
- una descrizione delle probabili conseguenze della violazione;
- una descrizione delle misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione e anche, se del caso, per attenuarne i possibili effetti negativi.

Come esempio di misure adottate per far fronte alla violazione e attenuarne i possibili effetti negativi, il titolare del trattamento può dichiarare che, dopo aver notificato la violazione all'autorità di controllo pertinente, ha ricevuto consigli sulla gestione della violazione e sull'attenuazione del suo impatto. Se del caso, il titolare del trattamento dovrebbe anche fornire consulenza specifica alle persone fisiche sul modo in cui proteggersi dalle possibili conseguenze negative della violazione, ad esempio reimpostando le password in caso di compromissione delle credenziali di accesso. Ancora una volta, il titolare del trattamento può scegliere di fornire informazioni supplementari rispetto a quanto richiesto qui.

Contattare l'interessato

In linea di principio, la violazione dovrebbe essere comunicata direttamente agli interessati coinvolti, a meno che ciò richieda uno sforzo sproporzionato. In tal caso, si procede a una comunicazione pubblica o a una misura simile che permetta di informare gli interessati con analoga efficacia (articolo 34, paragrafo 3, lettera c).

Nel comunicare una violazione agli interessati si devono utilizzare messaggi dedicati che non devono essere inviati insieme ad altre informazioni, quali aggiornamenti regolari, newsletter o messaggi standard. Ciò contribuisce a rendere la comunicazione della violazione chiara e trasparente.

Esempi di metodi trasparenti di comunicazione sono: la messaggistica diretta (ad esempio messaggi di posta elettronica, SMS, messaggio diretto), banner o notifiche su siti web di primo piano, comunicazioni

postali e pubblicità di rilievo sulla stampa. Una semplice comunicazione all'interno di un comunicato stampa o di un blog aziendale non costituirebbe un mezzo efficace per comunicare una violazione all'interessato. Il Gruppo di lavoro raccomanda al titolare del trattamento di scegliere un mezzo che massimizzi la possibilità di comunicare correttamente le informazioni a tutte le persone interessate. A seconda delle circostanze, ciò potrebbe significare che il titolare del trattamento dovrebbe utilizzare diversi metodi di comunicazione, anziché un singolo canale di contatto.

Inoltre il titolare del trattamento potrebbe dover garantire che la comunicazione sia accessibile in formati alternativi appropriati e lingue pertinenti al fine di assicurarsi che le persone fisiche siano in grado di comprendere le informazioni fornite loro. Ad esempio, nel comunicare una violazione a una persona, sarà di norma appropriata la lingua utilizzata durante il precedente normale corso degli scambi commerciali con il destinatario. Tuttavia, se la violazione riguarda interessati con i quali il titolare del trattamento non ha precedentemente interagito o, in particolare, interessati che risiedono in un altro Stato membro o in un altro paese non UE diverso da quello nel quale è stabilito il titolare del trattamento, la comunicazione nella lingua nazionale locale potrebbe essere accettabile, tenendo conto della risorsa richiesta. L'obiettivo principale è aiutare gli interessati a comprendere la natura della violazione e le misure che possono adottare per proteggersi.

Il titolare del trattamento è nella posizione migliore per stabilire il canale di contatto più appropriato per comunicare una violazione agli interessati, soprattutto se interagisce frequentemente con i suoi clienti. Tuttavia, è chiaro che il titolare del trattamento dovrebbe essere cauto nell'usare un canale di contatto compromesso dalla violazione, in quanto tale canale potrebbe essere utilizzato anche da autori di attacchi che si fanno passare per il titolare del trattamento.

Il titolare del trattamento potrebbe quindi contattare e consultare l'autorità di controllo non soltanto per chiedere consiglio sull'opportunità di informare gli interessati in merito a una violazione ai sensi dell'articolo 34, ma anche sui messaggi appropriati da inviare loro e sul modo più opportuno per contattarli.

Parallelamente, il considerando 88 indica che la notifica di una violazione dovrebbe tenere "conto dei legittimi interessi delle autorità incaricate dell'applicazione della legge, qualora una divulgazione prematura possa ostacolare inutilmente l'indagine sulle circostanze di una violazione di dati personali". Ciò può significare che in determinate circostanze, ove giustificato e su consiglio delle autorità incaricate dell'applicazione della legge, il titolare del trattamento può ritardare la comunicazione della violazione agli interessati fino a quando la comunicazione non pregiudica più tale indagine. Tuttavia, passato tale arco di tempo, gli interessati dovrebbero comunque essere tempestivamente informati.

Se non ha la possibilità di comunicare una violazione all'interessato perché non dispone di dati sufficienti per contattarlo, il titolare del trattamento dovrebbe informarlo non appena sia ragionevolmente possibile farlo (ad esempio quando l'interessato esercita il proprio diritto ai sensi dell'articolo 15 di accedere ai dati personali e fornisce al titolare del trattamento le informazioni supplementari necessarie per essere contattato).

Circostanze nelle quali non è richiesta la comunicazione

L'articolo 34, paragrafo 3, stabilisce tre condizioni che, se soddisfatte, non richiedono la comunicazione agli interessati in caso di violazione, ossia:

- il titolare del trattamento ha applicato misure tecniche e organizzative adeguate per proteggere i dati personali prima della violazione, in particolare misure atte a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi. Ciò potrebbe prevedere ad esempio la protezione dei dati personali con cifratura allo stato dell'arte oppure mediante tokenizzazione;
- immediatamente dopo una violazione, il titolare del trattamento ha adottato misure destinate a garantire che non sia più probabile che si concretizzi l'elevato rischio posto ai diritti e alle libertà delle persone fisiche. Ad esempio, a seconda delle circostanze del caso, il titolare del trattamento può aver immediatamente individuato e intrapreso un'azione contro il soggetto che ha avuto

accesso ai dati personali prima che questi fosse in grado di utilizzarli in qualsiasi modo. È necessario altresì tenere in debito conto delle possibili conseguenze di qualsiasi violazione della riservatezza, anche in questo caso, a seconda della natura dei dati in questione;

- contattare gli interessati richiederebbe uno sforzo sproporzionato, ad esempio nel caso in cui i dati di contatto siano stati persi a causa della violazione o non siano mai stati noti. Si pensi, ad esempio, al magazzino di un ufficio statistico che si è allagato e i documenti contenenti dati personali erano conservati soltanto in formato cartaceo. In tale circostanza il titolare del trattamento deve invece effettuare una comunicazione pubblica o prendere una misura analoga, tramite la quale gli interessati vengano informati in maniera altrettanto efficace. In caso di sforzo sproporzionato, si potrebbe altresì prevedere l'adozione di disposizioni tecniche per rendere le informazioni sulla violazione disponibili su richiesta, soluzione questa che potrebbe rivelarsi utile per le persone fisiche che potrebbero essere interessate da una violazione ma che il titolare del trattamento non può altrimenti contattare.

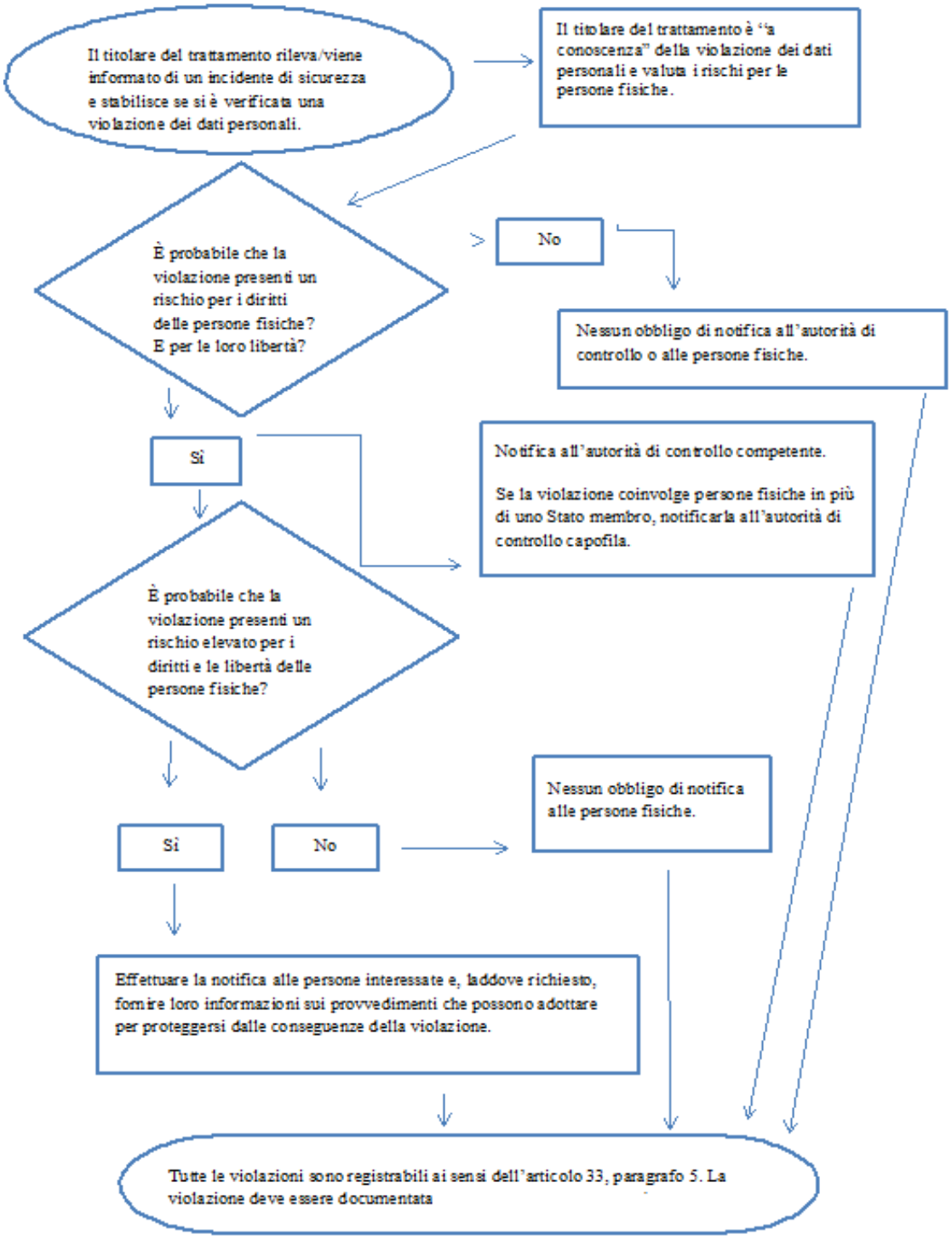
Conformemente al principio di responsabilizzazione, il titolare del trattamento dovrebbe essere in grado di dimostrare all'autorità di controllo di soddisfare una o più di queste condizioni. Va tenuto presente che, sebbene la comunicazione possa inizialmente non essere richiesta se non vi è alcun rischio per i diritti e le libertà delle persone fisiche, la situazione potrebbe cambiare nel corso del tempo e il rischio dovrebbe essere rivalutato.

Se il titolare del trattamento decide di non comunicare una violazione all'interessato, l'articolo 34, paragrafo 4, spiega che l'autorità di controllo può richiedere che lo faccia, qualora ritenga che la violazione possa presentare un rischio elevato per l'interessato. In alternativa, può ritenere che siano state soddisfatte le condizioni di cui all'articolo 34, paragrafo 3, nel qual caso la comunicazione all'interessato non è richiesta. Qualora stabilisca che la decisione di non effettuare la comunicazione all'interessato non sia fondata, l'autorità di controllo può prendere in considerazione l'esercizio dei poteri e delle sanzioni a sua disposizione.

ALLEGATI

Vengono di seguito riportate le istruzioni schematiche relative alla notifica della violazione (allegato A), ed una lista non esaustiva delle possibili violazioni (allegato B), come indicato dall'autorità Garante per la Protezione dei Dati Personali.

Allegato A: schematizzazione delle procedure di valutazione delle violazioni di dati personali



Allegato B: Esempi di violazioni dei dati personali e dei soggetti a cui notificarle

I seguenti esempi non esaustivi aiuteranno il titolare del trattamento a stabilire se deve effettuare la notifica in diversi scenari di violazione dei dati personali. Questi esempi possono altresì contribuire a distinguere tra rischio e rischio elevato per i diritti e le libertà delle persone fisiche.

Esempio	Notifica all'autorità di controllo?	Comunicazione all'interessato?	Note/raccomandazioni
Un titolare del trattamento ha effettuato un backup di un archivio di dati personali crittografati su una chiave USB. La chiave viene rubata durante un'effrazione.	No.	No.	Fintantoché i dati sono crittografati con un algoritmo all'avanguardia, esistono backup dei dati, la chiave univoca non viene compromessa e i dati possono essere ripristinati in tempo utile, potrebbe non trattarsi di una violazione da segnalare. Tuttavia, se la chiave viene successivamente compromessa, è necessaria la notifica.
ii. Un titolare del trattamento gestisce un servizio online. A seguito di un attacco informatico ai danni di tale servizio, i dati personali di persone fisiche vengono prelevati. Il titolare del trattamento ha clienti in un solo Stato membro.	Sì, segnalare l'evento all'autorità di controllo se vi sono probabili conseguenze per le persone fisiche.	Sì, segnalare l'evento alle persone fisiche a seconda della natura dei dati personali interessati e se la gravità delle probabili conseguenze per tali persone è elevata.	

iii. Una breve interruzione di corrente di alcuni minuti presso il call center di un titolare del trattamento impedisce ai clienti di chiamare il titolare del trattamento e accedere alle proprie registrazioni.	No.	No.	Questa non è una violazione soggetta a notifica, ma costituisce comunque un incidente registrabile ai sensi dell'articolo 33, paragrafo 5. Il titolare del trattamento deve conservare adeguate registrazioni in merito.
iv. Un titolare del trattamento subisce un	Sì, effettuare la segnalazione	Sì, effettuare la segnalazione alle	Se fosse stato disponibile un backup e i dati

attacco tramite *ransomware* che provoca la cifratura di tutti i dati. Non sono disponibili backup e i dati non possono essere ripristinati. Durante le indagini, diventa evidente che l'unica funzionalità dal *ransomware* era la cifratura dei dati e che non vi erano altri *malware* presenti nel sistema.	all'autorità di controllo, se vi sono probabili conseguenze per le persone fisiche in quanto si tratta di una perdita di disponibilità.	persone fisiche, a seconda della natura dei dati personali interessati e del possibile effetto della mancanza di disponibilità dei dati, nonché di altre possibili conseguenze.	avessero potuto essere ripristinati in tempo utile non sarebbe stato necessario segnalare la violazione all'autorità di controllo o alle persone fisiche, in quanto non si sarebbe verificata nessuna perdita permanente di disponibilità o di riservatezza. Tuttavia, qualora l'autorità di controllo fosse venuta a conoscenza dell'incidente con altri mezzi, avrebbe potuto prendere in considerazione lo svolgimento di un'indagine al fine di valutare il rispetto dei requisiti di sicurezza più ampi di cui all'articolo 32.

v. Una persona telefona al call center di una banca per segnalare una violazione dei dati. La persona ha ricevuto l'estratto conto mensile da un soggetto diverso. Il titolare del trattamento intraprende una breve indagine (ossia la conclude entro 24 ore) e stabilisce con ragionevole certezza che si è verificata una violazione dei dati personali e che vi è una potenziale carenza sistemica che potrebbe comportare il coinvolgimento già occorso o potenziale di altre persone fisiche.	Sì.	La comunicazione va effettuata soltanto alle persone fisiche coinvolte in caso di rischio elevato e se è evidente che altre persone fisiche non sono state interessate dall'evento.	Se dopo ulteriori indagini si stabilisce che l'evento ha interessato un numero maggiore di persone fisiche è necessario comunicare questo sviluppo all'autorità di controllo, e il titolare del trattamento deve informarne le altre persone fisiche interessate se sussiste un rischio elevato per loro.

vi. Un titolare del trattamento gestisce un mercato online e ha clienti in più Stati membri. Tale mercato subisce un attacco informatico a seguito del quale i nomi utente, le password e la cronologia degli acquisti vengono pubblicati online dall'autore dell'attacco.	Sì, segnalare l'evento all'autorità di controllo capofila se la violazione riguarda un trattamento transfrontaliero.	Sì, dato che la violazione potrebbe comportare un rischio elevato.	Il titolare del trattamento dovrebbe prendere delle misure, ad esempio forzare il ripristino delle password degli account interessati, e altri provvedimenti per attenuare il rischio. Il titolare del trattamento dovrebbe altresì considerare qualsiasi altro obbligo di notifica, ad esempio ai sensi della direttiva NIS, trattandosi di un fornitore di servizi digitali.

vii. Una società di *hosting* di siti web che funge da responsabile del trattamento individua un errore nel codice che controlla l'autorizzazione dell'utente. A causa di tale vizio, qualsiasi utente può accedere ai dettagli dell'account di qualsiasi altro utente.	In veste di responsabile del trattamento, la società di *hosting* di siti web deve effettuare la notifica ai clienti interessati (i titolari del trattamento) senza ingiustificato ritardo. Supponendo che la società di *hosting* di siti web abbia condotto le proprie indagini, i titolari del trattamento interessati dovrebbero essere ragionevolmente certi di aver subito una violazione e pertanto è probabile che vengano considerati "a conoscenza" della violazione nel momento in cui hanno ricevuto la notifica da parte della società di *hosting* (il responsabile del trattamento). Il titolare del trattamento deve quindi effettuare la notifica all'autorità di controllo.	Qualora non vi siano probabili rischi elevati per le persone fisiche non è necessario effettuare una comunicazione a tali persone.	La società di *hosting* di siti web (responsabile del trattamento) deve prendere in considerazione qualsiasi altro obbligo di notifica (ad esempio ai sensi della direttiva NIS, trattandosi di un fornitore di servizi digitali). Qualora non vi sia alcuna prova che tale vulnerabilità sia sfruttata presso uno dei suoi titolari del trattamento, la violazione potrebbe non essere soggetta all'obbligo di notifica, tuttavia potrebbe essere una violazione da registrare o essere il segno di un mancato rispetto dell'articolo 32.

viii. Le cartelle cliniche di un ospedale sono indisponibili per un periodo di 30 ore a causa di un attacco informatico.	Sì, l'ospedale è tenuto a effettuare la notifica in quanto può verificarsi un rischio elevato per la salute e la tutela della vita privata dei pazienti.	Sì, informare le persone fisiche coinvolte.	
ix. I dati personali di un gran numero di studenti vengono inviati per errore a una mailing list sbagliata con più di 1 000 destinatari.	Sì, segnalare l'evento all'autorità di controllo.	Sì, segnalare l'evento alle persone fisiche coinvolte in base alla portata e al tipo di dati personali coinvolti e alla gravità delle possibili conseguenze.	
x. Una e-mail di marketing diretto viene inviata ai destinatari nei campi "a:" o "cc:", consentendo così a ciascun destinatario di vedere l'indirizzo e- mail di altri destinatari.	Sì, la notifica all'autorità di controllo può essere obbligatoria se è interessato un numero elevato di persone, se vengono rivelati dati sensibili (ad esempio una mailing list di uno psicoterapeuta) o se altri fattori presentano rischi elevati (ad esempio, il messaggio di posta elettronica contiene le password iniziali).	Sì, segnalare l'evento alle persone fisiche coinvolte in base alla portata e al tipo di dati personali coinvolti e alla gravità delle possibili conseguenze.	La notifica potrebbe non essere necessaria se non vengono rivelati dati sensibili e se viene rivelato soltanto un numero limitato di indirizzi di posta elettronica.

Quartu Sant'Elena, 03/04/24

Il Dirigente Scolastico

Prof. Massimo Mocci

Documento informatico firmato digitalmente ai sensi del D.Lgs 82/2005 s.m.i. e norme collegate, il quale sostituisce il documento cartaceo e la firma autografa

Liceo Classico Linguistico e Scienze Umane B.R. Motzo

Sede: Via Don Sturzo, 4, 09045 Quartu Sant'Elena (CA)
Telefono: 070/825629 **Sito istituzionale:** liceomotzo.edu.it
E-mail: CAPC09000E@istruzione.it **PEC:** CAPC09000E@pec.istruzione.it
C.U.: UFAGLG **C.F.:** 92168540927

Regolamento: procedure di pubblicazione all'albo on line

Articolo 1: Oggetto e contesto normativo

Il presente Regolamento disciplina la tenuta, il funzionamento e le responsabilità relative alle pubblicazioni nell' Albo on-line dell'Istituto. Tali attività saranno svolte nel rispetto dei principi di Pubblicità e di Trasparenza Amministrativa previste da:

- articolo 1, della Legge n. 241 del 07.08.1990 e seguenti modifiche e integrazioni
- articolo 32, comma 1, della Legge 18-6-2009, n. 69. che reca disposizioni dirette alla eliminazione degli sprechi relativi al mantenimento di documenti in forma cartacea
- Delibera Anac n. 1309 del 28 dicembre 2016 relativa all'accesso agli atti amministrativi.

Articolo 2 Finalità

La pubblicazione di atti all'Albo on-line è finalizzata a fornire presunzione di conoscenza legale degli stessi, a qualunque effetto giuridico specifico essa assolva (pubblicità, notizia dichiarativa, costitutiva, integrativa dell'efficacia, ecc.). Secondo l'art. 32 della L. 69/2009, gli obblighi di pubblicazione di atti e provvedimenti amministrativi aventi effetto di pubblicità legale sono assolti con la pubblicazione nella sezione Albo del sito web istituzionale dell'amministrazione. A decorrere dal 1° gennaio 2011 non esistono altre modalità di conseguire le finalità di pubblicità degli atti della pubblica amministrazione e non viene riconosciuto alcun valore legale alle pubblicazioni su eventuali albi cartacei.

Articolo 3 Modalità di accesso al servizio on - line

Secondo quanto disposto dalla vigente normativa è possibile accedere al servizio digitale "Albo on-line" attraverso un link posto sulla home page del sito web della scuola e precisamente nell'area denominata Pubblicità legale.

Articolo 4 Atti soggetti alla pubblicazione

Sono soggetti alla pubblicazione all'Albo on-line tutti gli atti per i quali la legge ne preveda l'adempimento. Gli atti che vengono pubblicati possono essere interni all'ente oppure provenire da altri enti esterni o da soggetti privati. Gli atti interni sono pubblicati nella loro versione integrale, fatto salve parti omesse per rispetto della privacy, e conforme all'originale, ivi compresi i relativi allegati (le delibere degli organi collegiali verranno pubblicate tramite estratto del verbale).

Si elencano, a titolo meramente esemplificativo e non esaustivo, i principali atti che vengono pubblicati on line:

1.Delibere

- Consiglio d'Istituto

2.Bandi di gare

- Assistenza tecnica
- Compagnie di Assicurazione
- Noleggio Pullman
- Istituto Cassiere
- Acquisti materiale

3.Comunicazioni

- Sindacali (circolari scioperi e assemblee)
- Famiglie

4.Convocazioni

- Consiglio di Istituto
- Giunta Esecutiva
- Collegio Docenti
- Assemblee genitori
- Assemblee sindacali
- Individuazioni aspiranti supplenze

5.Contabilità

- Programma annuale
- Conto Consuntivo
- Variazioni al Programma Annuale

6.Graduatorie

- Graduatorie interne
- Graduatorie docenti
- Graduatorie ATA

7.Contratti ed individuazioni

- Individuazione per nomina personale non a tempo indeterminato
- Esperti esterni

8.Altro

- Atti suscettibili di pubblicazione

Articolo 4: Atti non soggetti alla pubblicazione

Non sono soggetti alla pubblicazione ai sensi del precedente articolo gli atti e i documenti cui l'adempimento non produca effetti legali. In tal caso tali documenti possono essere collocati in altre sezioni del sito internet istituzionale.

Articolo 5 Modalità di pubblicazione

I documenti restano pubblicati per il tempo stabilito dalle singole disposizioni di legge o di regolamento. Salvo casi specifici la durata è di quindici giorni.
La pubblicazione avviene per giorni interi, naturali e consecutivi, comprese le festività civili.
Durante il periodo di pubblicazione è vietato sostituire e/o modificare, informalmente, il contenuto dei documenti ma le eventuali modifiche apportate devono risultare dallo stesso documento sostituito o modificato ovvero da altro atto allegato allo stesso. Di norma il termine di pubblicazione ricomincia a decorrere ex novo dalla data dell'avvenuta sostituzione o modifica.
L'Albo Pretorio on-line deve essere accessibile in tutti i giorni dell'anno, salvo interruzioni determinate da cause di forza maggiore. Alla scadenza dei termini gli atti già pubblicati non sono più visionabili. La pubblicazione sul web deve garantire il "diritto all'oblio" dei soggetti coinvolti e concluso il periodo di affissione i dati devono scomparire. Il diritto all'oblio è altresì garantito da misure tecniche che impediscono l'indicizzazione dei contenuti nei motori di ricerca.

Art. 6 Pubblicazione degli atti formati dall'Ente

Il Responsabile del procedimento che ha adottato l'atto provvede a richiedere la pubblicazione all'albo in formato elettronico non modificabile (PDF) e firmato digitalmente.
La pubblicità legale si realizza quando sono garantite:

- la autenticità dell'atto pubblicato
- la conformità all'originale
- inalterabilità (presupposto per garantire la integrità)
- preservare il grado giuridico dell'atto
- possibilità di conservazione
- rispettare i requisiti di accessibilità e usabilità

Art. 7 Pubblicazione degli atti per conto di soggetti esterni all'Ente

L'Istituto provvede alla pubblicazione all'Albo pretorio informatico di documenti provenienti da altre pubbliche amministrazione o da altri soggetti abilitati tramite l'emanazione di un atto o decreto di pubblicazione (es. graduatorie).

Art. 8- Registro degli atti pubblicati

Tutti i documenti inseriti sono numerati in ordine cronologico in base alla data e l'ora di inserimento nell'albo. Il numero progressivo univoco per anno viene generato automaticamente dal sistema. Tutto ciò che dovrà essere affisso all'albo deve essere protocollato. A tal fine le circolari di servizio recanti atti da pubblicare all'albo vanno protocollate.

Articolo 9 -Integralità della pubblicazione

Gli atti sono, fatto salve parti omesse per rispetto della privacy, pubblicati nel loro integrale contenuto, comprensivo di tutti gli allegati.

Articolo 10 - Modalità di redazione degli atti

Nel predisporre le proposte di deliberazione, le determinazioni ed ogni altro atto destinato alla diffusione mediante pubblicazione sul sito internet dell'Istituzione Scolastica, il personale di segreteria che genera l'atto deve attenersi scrupolosamente ai principi della necessità e proporzionalità delle informazioni concernenti dati personali fornite dall'atto, nel pieno rispetto della legge sulla Privacy. Per necessità e proporzionalità si intende che chi genera l'atto deve indicare nello stesso, solo ed esclusivamente quelle informazioni che possono essere ritenute rilevanti ed indispensabili al fine della comprensione della fattispecie e della congruità della motivazione ed al fine di consentire agli eventuali interessati e contro interessati all'atto, la conoscenza necessaria e

sufficiente per esercitare, rispettivamente, la funzione di controllo e la tutela dei propri diritti e/o interessi legittimi.

Articolo 11 Figure Responsabili: Responsabile Procedimento e Responsabile Pubblicazione

La responsabilità della formazione dell'atto soggetto a pubblicità legale è del **Responsabile del procedimento** che ha generato l'atto e la responsabilità di pubblicazione sull'albo on line è del **Responsabile della pubblicazione** che può a sua volta delegare tali adempimenti ad altri soggetti competenti.
Al Responsabile della pubblicazione compete anche la possibilità di annullamento di un documento che comunque deve rimanere in pubblicazione per il periodo indicato e riportare la dicitura "annullato". I documenti annullati devono essere compresi nel Repertorio di pubblicazione.
Il Responsabile della pubblicazione nel caso in cui un documento informatico sia stato ottenuto come copia per immagine del cartaceo originale, per rispondere ai requisiti di accessibilità, dovrà associare all'immagine una descrizione testuale alternativa. I Responsabili del procedimento hanno l'obbligo di:

1. caricare il documento in formato elettronico;
2. assicurarsi che saranno pubblicati in un formato non modificabile da terzi;
3. porre attenzione alle informazioni che contengono dati personali di natura sensibile o giudiziari che saranno sostituiti da opportuni omissis.
4. assicurarsi che la consultazione degli atti pubblicati riportano chiare e ben visibili:
   a) il numero di protocollo generale;
   b) la data di pubblicazione;
   c) la descrizione o l'oggetto del documento;

Articolo 12 Garanzie di riservatezza

1. La pubblicazione degli atti all'albo, salve e impregiudicate le garanzie previste dalla legge 7-8-1990, n. 241 in tema di accesso ai documenti amministrativi, avviene nel rispetto della tutela alla riservatezza dei cittadini, secondo quanto disposto dal decreto legislativo 30-6-2003, n. 196 e Regolamento UE 679/2016, in materia di protezione dei dati personali.
2. L'accesso agli atti pubblicati all'Albo Pretorio on-line dovrà essere consentito in modalità di sola lettura, al fine di evitare che gli stessi possano essere modificati o cancellati dallo spazio "web". Potranno essere scaricabili dall'Albo Pretorio online gli atti pubblicati in un formato elettronico tale da impedire qualsiasi alterazione del medesimo.
3. Le modalità di pubblicazione all'Albo Pretorio on-line degli atti e documenti contenenti dati personali, devono avere caratteristiche di sicurezza ed inviolabilità conformi alle misure previste dall'art.51 del D.Lgs. n° 82/2005.
4. La pubblicazione di atti all'Albo Pretorio on-line, costituendo operazione di trattamento di dati personali, consistente, nella diffusione degli stessi dati, deve essere espletata nel rispetto delle specifiche norme previste dal Regolamento UE 679/2016 e dal D.Lgs 196/2003:
   - tutti i dati personali possono essere oggetto di una o più operazioni di trattamento purché finalizzate allo svolgimento di funzioni istituzionali e nel rispetto dei presupposti e dei limiti previsti dal D.Lgs. 196/2003, Dal Regolamento UE 679/2016, da ogni altra disposizione di legge o di regolamento, dai provvedimenti del Garante per la privacy, di cui principalmente la deliberazione n° 17 del 19.04.2007 "Linee guida in materia di trattamento di dati personali contenuti anche in atti e documenti amministrativi effettuato da soggetti pubblici per finalità di pubblicazione e diffusione sul web" (cui si rinvia e consultabile al sito: https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/1407101);

- sono da rispettare i principi di necessità e di proporzionalità dei dati personali diffusi rispetto alla finalità della pubblicità-notizia che con la pubblicazione si persegue;
- la diffusione dei dati sensibili e giudiziari è lecita se la stessa sia realmente indispensabile e pertinente rispetto al contenuto del provvedimento e non eccedente rispetto al fine che con esso si intende perseguire, in conformità all'apposito Regolamento per il trattamento dei dati sensibili e giudiziari approvato con Decreto Ministeriale n. 305 del 7 Dicembre 2006;
- i dati sensibili e giudiziari possono essere oggetto di diffusione, soltanto se tale operazione di trattamento sia prevista da una norma di legge o dall'apposito Regolamento approvato dal Ministero della P. I. già citato;
- i dati idonei a rivelare lo stato di salute non possono mai essere diffusi;
- i dati personali diversi dai dati sensibili e giudiziari possono essere oggetto di diffusione se siffatta operazione di trattamento sia prevista da una norma di legge o di regolamento;

5. Al contenuto integrale degli atti sarà comunque consentito l'accesso da parte dei soggetti titolari di un interesse diretto, concreto e attuale, corrispondente ad una situazione giuridicamente tutelata e collegata al documento al quale è richiesto l'accesso come previsto dall'art. 22 della legge n° 241/1990 e dall'art. 2 del D.P.R. n° 184/2006.
6. Il rispetto dei principi e delle disposizioni in materia di riservatezza dei dati personali, anche in relazione alla pubblicazione obbligatoria all'Albo Pretorio informatico, è assicurato con idonee misure o accorgimenti tecnici da attuare in sede di redazione dell'atto stesso da parte del Responsabile che genera il medesimo atto, pertanto, del contenuto degli atti pubblicati, in relazione al rispetto delle norme per la protezione dei dati personali, anche con riguardo alla loro diffusione per mezzo della pubblicazione dei rispettivi atti all'Albo Pretorio on-line, è responsabile l'incaricato che genera l'atto.

Quartu Sant'Elena, 03/04/24

Il Dirigente Scolastico
Prof. Massimo Mocci

Documento informatico firmato digitalmente ai sensi del D.Lgs 82/2005 s.m.i. e norme collegate, il quale sostituisce il documento cartaceo e la firma autografa

Liceo Classico Linguistico e Scienze Umane B.R. Motzo

Sede: Via Don Sturzo, 4, 09045 Quartu Sant'Elena (CA)
Telefono: 070/825629 **Sito istituzionale:** liceomotzo.edu.it
E-mail: CAPC09000E@istruzione.it **PEC:** CAPC09000E@pec.istruzione.it
C.U.: UFAGLG **C.F.:** 92168540927

Allegato III: Regolamento concernente gli obblighi di pubblicità e trasparenza in attuazione del D. Lgs 33 del 14/3/2013 come modificato dal D. Lgs 97/2016

Capo I
Principi generali

Art. 1: Oggetto e contesto normativo

1.1

Il presente Regolamento disciplina la tenuta, il funzionamento e le responsabilità relative alle pubblicazioni nella sezione Amministrazione Trasparente (AT) di cui all'**art. 9 del decreto legislativo 14 marzo 2013, n. 33** che prevede:

- L'istituzione di una sezione "Amministrazione trasparente" accessibile dalla home page del sito web istituzionale ed in cui devono essere pubblicati i dati, le informazioni e i documenti ai sensi della normativa vigente (e specificati in modo puntuale negli articoli seguenti del presente regolamento).
- Al fine di evitare eventuali duplicazioni, la suddetta pubblicazione può essere sostituita da un collegamento ipertestuale alla sezione del sito in cui sono presenti i relativi dati, informazioni o documenti assicurando la qualità delle informazioni
- Le amministrazioni non possono disporre filtri e altre soluzioni tecniche atte ad impedire ai motori di ricerca web di indicizzare ed effettuare ricerche all'interno della sezione AT

1.2

Per l'applicazione alle istituzioni scolastiche delle disposizioni di cui alla legge 190/2012 e 33/2013 è intervenuta il 13 aprile 2016, con delibera n. 430, l'Autorità Nazionale Anticorruzione adottando le *"Linee guida sull'applicazione alle istituzioni scolastiche delle disposizioni di cui alla legge 6 novembre 2012, n. 190 e al decreto legislativo 14 marzo 2013, n. 33"*. Con le menzionate Linee guida vengono fornite indicazioni volte a orientare le istituzioni scolastiche nell'applicazione della normativa in materia di prevenzione della corruzione e trasparenza, tenuto conto delle caratteristiche organizzative e dimensionali del settore dell'istruzione scolastica e delle singole istituzioni, della specificità e peculiarità delle funzioni, nonché della disciplina di settore che caratterizza queste amministrazioni.

Art. 2: Finalità

2.1

La pubblicazione di dati, informazioni e documenti in Amministrazione Trasparente è finalizzata a garantire la **trasparenza intesa come accessibilità totale** ai dati e ai documenti in possesso della pubblica amministrazione. Ha lo scopo di tutelare i diritti dei cittadini e di promuovere partecipazione e forme diffuse di controllo sulle attività delle istituzioni e sull'utilizzo delle risorse pubbliche.

2.2

La pubblicazione dei dati in possesso delle pubbliche amministrazioni intende incentivare la partecipazione dei cittadini allo scopo di:

- assicurare la conoscenza dei servizi resi, le caratteristiche quantitative e qualitative e le modalità di erogazione;
- prevenire fenomeni di corruzione e promuovere l'integrità;
- sottoporre al controllo diffuso ogni fase del ciclo di gestione della performance per consentirne il miglioramento.

Art. 3: Pubblicità, diritto alla conoscibilità e riutilizzabilità

3.1

I documenti, le informazioni e i dati oggetto di pubblicazione obbligatoria ai sensi del presente regolamento sono pubblici e chiunque ha diritto di conoscerli, di fruirne gratuitamente e di utilizzarli, citandone la fonte e rispettandone l'integrità, alle condizioni previste dalla normativa vigente sul riutilizzo di documenti nel settore pubblico di cui al decreto legislativo 24 gennaio 2006, n. 36. I dati personali sono riutilizzabili in termini compatibili con gli scopi per i quali sono stati raccolti e registrati e nel rispetto del Regolamento UE 679/2016.

Art. 4: Limiti alla trasparenza

4.1

Nel predisporre le proposte di deliberazione, le determinazioni ed ogni altro atto destinato alla diffusione mediante pubblicazione sul sito internet dell'Istituzione Scolastica, il personale amministrativo che genera l'atto deve attenersi scrupolosamente ai principi della necessità e proporzionalità delle informazioni concernenti dati personali fornite dall'atto, nel pieno rispetto della legge sulla Privacy. Per **necessità e proporzionalità** si intende che chi genera l'atto deve indicare nello stesso solo ed esclusivamente quei dati personali che sono rilevanti al fine del conseguimento della finalità della pubblicazione provvedendo a rendere non intelligibili i dati personali non pertinenti o non indispensabili rispetto alle specifiche finalità di trasparenza della pubblicazione.

4.2

La diffusione dei **dati sensibili e giudiziari** è lecita se la stessa è prevista da una norma di legge ed è realmente indispensabile e pertinente rispetto al contenuto del provvedimento e non eccedente rispetto al fine che con esso si intende perseguire, in conformità all'apposito Regolamento per il trattamento dei dati sensibili e giudiziari approvato con Decreto Ministeriale n. 305 del 7 Dicembre 2006;

4.2

L'incaricato della pubblicazione di cui all'art. 28 del presente regolamento, prima della diffusione del documento in AT, dovrà provvedere a rendere non intelligibili i dati personali non pertinenti o non indispensabili rispetto alle specifiche finalità di trasparenza della pubblicazione.

Art. 5: Pubblicazione di documenti non soggetti ad obbligo di pubblicità

5.1

L'Istituto può disporre la pubblicazione nel proprio sito istituzionale ed in AT di dati, informazioni e documenti che non ha l'obbligo di pubblicare ai sensi del presente regolamento, fermi restando i limiti e le condizioni espressamente previsti da disposizioni di legge, procedendo alla anonimizzazione dei dati personali eventualmente presenti. La pubblicazione di documenti non soggetti ad obbligo di pubblicità può avvenire in ***Amministrazione Trasparente/ Altri contenuti / Dati ulteriori***.

Art. 6: Qualità delle informazioni

6.1

Deve essere garantita la qualità delle informazioni riportate nel sito istituzionale nel rispetto degli obblighi di pubblicazione, assicurandone l'integrità, il costante aggiornamento, la completezza, la tempestività, la semplicità di consultazione, la comprensibilità, l'omogeneità, la facile accessibilità, nonché la conformità ai documenti originali in possesso dell'Istituto, l'indicazione della loro provenienza e la loro riutilizzabilità.

6.2

L’esigenza di assicurare adeguata qualità delle informazioni diffuse non può, in ogni caso, costituire motivo per l’omessa o ritardata pubblicazione dei dati, delle informazioni e dei documenti

Art. 7: Modalità di pubblicazione

7.1

Le modalità di pubblicazione in AT degli atti e documenti contenenti dati personali, devono avere caratteristiche di sicurezza ed inviolabilità conformi alle misure previste dall’art.51 del D.Lgs. n° 82/2005.

7.2

I documenti oggetto di pubblicazione in AT sono di norma in formato elettronico non modificabile (PDF) e firmati digitalmente.

Art. 8: Decorrenza e durata dell’obbligo di pubblicazione

8.1

I documenti contenenti atti oggetto di pubblicazione obbligatoria ai sensi del presente regolamento sono pubblicati tempestivamente e in ogni caso non oltre i tre mesi decorrenti dalla formazione dell’atto, sul sito istituzionale dell’Autorità.

8.2

I documenti contenenti altre informazioni e dati oggetto di pubblicazione obbligatoria sono mantenuti aggiornati con cadenza annuale.

8.3

I dati, informazioni e documenti di cui all’art. 14, c. 2 del D. Lgs 33/2013 sono pubblicati in ***AT/personale/titolari di incarichi dirigenziali*** entro tre mesi dalla nomina e per i tre anni successivi dalla cessazione dell'incarico del dirigente scolastico (vedere art. 12 del presente regolamento).

8.4

I dati, informazioni e documenti di cui all’art. 15, commi 1 e 2 del D. Lgs 33/2013 (incarichi di collaborazione e consulenza) sono pubblicati in ***AT/consulenti e collaboratori/titolari di incarichi di collaborazione e consulenza*** entro tre mesi dal conferimento dell’incarico e per i tre anni successivi dalla cessazione dell'incarico (vedere art. 12 del presente regolamento).

8.5

In mancanza di specifica disposizione i contenuti ad obbligo di pubblicazione in AT saranno pubblicati per **5 anni** a partire dal primo gennaio dell’anno successivo a quello di pubblicazione.

8.6

In ottemperanza a disposizioni di leggi specifiche, differenti tempi di pubblicazione potranno essere stabiliti con separata deliberazione, anche per categorie di dati e tenuto conto delle specifiche finalità di pubblicazione, a decorrere dal 1 gennaio dell’anno successivo a quello da cui decorre l’obbligo di pubblicazione e, in ogni caso, fino a che gli atti pubblicati producono i loro effetti.

Art. 9: Scadenza dei termini di pubblicazione

9.1

Alla scadenza del termine di durata dell’obbligo di pubblicazione stabilito agli artt. 7.3, 7.4, 7.5 o di altra separata deliberazione i documenti, le informazioni e i dati sono cancellati dal sito e da amministrazione trasparente.

9.2

E’ possibile, dopo la scadenza dei termini di pubblicazione, spostare i contenuti del sito e di amministrazione trasparente in appositi archivi che non potranno però essere accessibili al pubblico se non per documenti privi di dati personali o anonimizzati.

Capo II

I contenuti di Amministrazione Trasparente

Art. 10: Obblighi di pubblicazione concernenti gli atti di carattere normativo e amministrativo generale

10.1

E' pubblicato in ***AT/ Disposizioni generali/ Piano triennale per la prevenzione della corruzione e della trasparenza (PTPCT)*** il link al PTPCT redatto dall'Ufficio Scolastico della regione nel suo ruolo di Responsabile Prevenzione Corruzione e per la Trasparenza (RPCT) degli istituti scolastici sul proprio territorio.

10.2

Sono pubblicati in ***AT/ Disposizioni generali/ Atti generali*** i riferimenti normativi, con i relativi link alle norme di legge che ne regolano l'istituzione, l'organizzazione e l'attività. Sono altresì pubblicati le comunicazioni, i regolamenti e le istruzioni emanati dall'istituto e ogni atto che dispone in generale sull'organizzazione, sulle funzioni, sugli obiettivi, sui procedimenti ovvero nei quali si determina l'interpretazione di norme giuridiche che riguardano i compiti istituzionali dell'istituto o si dettano disposizioni per l'applicazione di esse, ivi compresi i codici di condotta.

Art. 11: Obblighi di pubblicazione concernenti l'organizzazione dell'Amministrazione

11.1

Sono pubblicate in ***AT/ Organizzazione*** le informazioni e i dati concernenti la propria organizzazione, corredati dai documenti anche normativi di riferimento. Sono pubblicati fra gli altri:

a) componenti del Consiglio di Istituto;
b) articolazione degli uffici, organigramma, competenze e risorse a disposizione di ciascun ufficio;
c) elenco dei numeri di telefono nonché caselle di posta elettronica istituzionali e caselle di posta elettronica certificata dedicate

Art. 12: Obblighi di pubblicazione concernenti i titolari di incarichi di collaborazione o consulenza

12.1

In ***AT/Consulenti e collaboratori*** sono pubblicati gli estremi degli atti di conferimento di incarichi di collaborazione o di consulenza a soggetti esterni a qualsiasi titolo (compresi quelli affidati con contratto di collaborazione coordinata e continuativa) per i quali è previsto un compenso con indicazione dei soggetti percettori, della ragione dell'incarico e dell'ammontare erogato.

Per ciascun titolare di incarico sono pubblicati:

- curriculum, redatto in conformità al vigente modello europeo;
- compensi comunque denominati, relativi al rapporto di lavoro, di consulenza o di collaborazione;
- dati relativi allo svolgimento di incarichi o alla titolarità di cariche in enti di diritto privato regolati o finanziati dalla pubblica amministrazione o allo svolgimento di attività professionali;

Sono altresì pubblicate tabelle di sintesi relative agli elenchi dei consulenti con indicazione di oggetto, durata e compenso dell'incarico (comunicate alla Funzione pubblica); attestazione dell'avvenuta verifica dell'insussistenza di situazioni, anche potenziali, di conflitto di interesse

Art. 13: Obblighi di pubblicazione concernenti i titolari di incarichi dirigenziali

13.1

In ***AT/Personale/Dirigenti*** sono pubblicati gli estremi degli atti di conferimento di incarichi dirigenziali a soggetti dipendenti della pubblica amministrazione. Relativamente al Dirigente Scolastico in carica sono pubblicati:

- Curriculum, redatto in conformità al vigente modello europeo
- compensi, comunque denominati, relativi al rapporto di lavoro, con specifica evidenza delle eventuali componenti variabili o legate alla valutazione del risultato, e a incarichi di consulenza e collaborazione da parte dell'amministrazione di appartenenza o di altro soggetto
- dati relativi allo svolgimento di incarichi o alla titolarità di cariche in enti di diritto privato regolati o finanziati dalla pubblica amministrazione o allo svolgimento di attività professionali, e relativi compensi
- dichiarazione sulla insussistenza di una delle cause di inconferibilità dell'incarico
- dichiarazione sulla insussistenza di una delle cause di incompatibilità al conferimento dell'incarico

13.2
In ***AT/Personale/Dirigenti cessati*** per i tre anni successivi dalla cessazione dell'incarico sono pubblicati i curricula dei dirigenti cessati.

Art. 14: Obblighi di pubblicazione concernenti la dotazione organica e il costo del personale

14.1
L'Istituto rende accessibili su **AT/Personale** le informazioni relative a:

- Dotazione organica (numero di dipendenti suddivisi per personale docente ed ATA)
- Personale non a tempo indeterminato
- Tassi di assenza del personale
- Incarichi conferiti o autorizzati ai dipendenti
- Contrattazione collettiva
- Contrattazione integrativa

14.2
Le informazioni di cui al punto precedente potranno essere accessibili da amministrazione trasparente anche attraverso link che riconducono a piattaforme esterne quali ***scuola in chiaro***, ***operazione trasparenza***, ***contrattiintegrativipa.it***, ***aranagenzia.it*** e ***consulentipubblici.gov.it***.

Art. 15: Obblighi di pubblicazione dei dati relativi alla valutazione della performance e all'attribuzione di premi al personale

15.1
In **AT/Performance/Ammontare complessivo dei premi** è resa pubblica la distribuzione del trattamento accessorio, in forma aggregata, al fine di dare conto del livello di selettività utilizzato nella distribuzione dei premi e degli incentivi (MOF)

15.2
In **AT/Performance/Dati relativi ai premi** sono resi noti i criteri per la distribuzione dei premi ed il grado di differenziazione dell'utilizzo della premialità sia per i dirigenti sia per i dipendenti.

Art. 16: Obblighi di pubblicazione su attività e procedimenti

16.1
In **AT/Attività e procedimenti/Dati aggregati attività amministrativa** sono riportate in formato tabellare le seguenti informazioni per ciascuna tipologia di procedimento:

1. breve descrizione del procedimento
2. unità organizzative responsabili dell'istruttoria
3. nome del responsabile del procedimento e relativi recapiti
4. ove diverso, il responsabile del provvedimento finale e relativi recapiti
5. modalità con le quali gli interessati possono ottenere le informazioni relative ai procedimenti in corso che li riguardino
6. termine fissato in sede di disciplina normativa del procedimento per la conclusione con l'adozione di un provvedimento espresso
7. Documenti da allegare all'istanza e modulistica
8. link di accesso al servizio on line, ove sia già disponibile in rete, o tempi previsti per la sua attivazione
9. modalità per l'effettuazione dei pagamenti eventualmente necessari
10. nome del soggetto a cui è attribuito, in caso di inerzia, il potere sostitutivo, nonchè modalità per attivare tale potere, con indicazione dei recapiti telefonici e delle caselle di posta elettronica istituzionale

16.2
In **AT/Attività e procedimenti/Dichiarazioni sostitutive e acquisizione d'ufficio dei dati** sono riportati i recapiti telefonici e casella di posta elettronica istituzionale dell'ufficio responsabile per le attività volte a gestire, garantire e verificare la trasmissione dei dati o l'accesso diretto degli stessi da parte delle amministrazioni procedenti all'acquisizione d'ufficio dei dati e allo svolgimento dei controlli sulle dichiarazioni sostitutive.

Art. 17: Obblighi di pubblicazione dei Provvedimenti

17.1
In **AT/Provvedimenti/ Provvedimenti organi indirizzo politico** deve essere riportato l'elenco dei provvedimenti del Consiglio di Istituto con particolare riferimento ai provvedimenti finali dei procedimenti di: scelta del contraente per l'affidamento di lavori, forniture e servizi, anche con riferimento alla modalità di selezione prescelta (anche

attraverso link alla sotto-sezione "bandi di gara e contratti"); accordi stipulati dall'amministrazione con soggetti privati o con altre amministrazioni pubbliche. L'aggiornamento dell'elenco delle delibere del Consiglio di Istituto avviene con cadenza semestrale.

17.2
In **AT/Provvedimenti/ Provvedimenti dirigenti** è riportato l'elenco dei provvedimenti del Dirigente Scolastico, con particolare riferimento ai provvedimenti finali dei procedimenti di: scelta del contraente per l'affidamento di lavori, forniture e servizi, anche con riferimento alla modalità di selezione prescelta (anche attraverso link alla sotto-sezione "bandi di gara e contratti"); accordi stipulati dall'amministrazione con soggetti privati o con altre amministrazioni pubbliche. L'aggiornamento dell'elenco delle determine del Dirigente Scolastico avviene con cadenza semestrale.

Art. 18: Obblighi di pubblicazione informazioni bandi di gara e contratti

18.1
In **AT/Bandi di gara e contratti/ Informazioni sulle singole procedure in formato tabellare** sono pubblicate con cadenza annuale tabelle riassuntive rese liberamente scaricabili in un formato digitale standard aperto con informazioni sui contratti relative all'anno precedente (nello specifico: Codice Identificativo Gara (CIG), struttura proponente, oggetto del bando, procedura di scelta del contraente, elenco degli operatori invitati a presentare offerte/numero di offerenti che hanno partecipato al procedimento, aggiudicatario, importo di aggiudicazione, tempi di completamento dell'opera servizio o fornitura, importo delle somme liquidate)

18.2
In **AT/Bandi di gara e contratti/ Atti delle amministrazioni aggiudicatrici e degli enti aggiudicatori distintamente per ogni procedura** sono pubblicate tempestivamente per ogni procedura di affidamento di lavori, servizi e forniture:

- Avviso di preinformazione
- Delibera a contrarre
- Avvisi, bandi e inviti per contratti di lavori, servizi e forniture sottosoglia comunitaria
- Avvisi, bandi e inviti per contratti di lavori, servizi e forniture soprasoglia comunitaria
- Bandi e avvisi per appalti di lavori, servizi e forniture nei settori speciali
- Avviso sui risultati della procedura di affidamento
- Avvisi periodici indicativi e avvisi sull'esistenza di un sistema di qualificazione - settori speciali
- Determina di affidamento
- Relativamente ai procedimenti di cui all'art. 1, comma 16, lett. b, della legge 6 novembre 2012, n. 190:
    - la struttura proponente;
    - l'oggetto del bando;
    - l'elenco degli operatori invitati a presentare offerte;
    - l'aggiudicatario;
    - l'importo di aggiudicazione;
    - i tempi di completamento dell'opera, servizio o fornitura;
    - l'importo delle somme liquidate

Art. 19: Sovvenzioni, contributi, sussidi, vantaggi economici

19.1
In **AT/ Sovvenzioni, contributi, sussidi, vantaggi economici / Criteri e modalità** sono resi pubblici gli atti con i quali sono determinati i criteri e le modalità cui l'amministrazione si attiene per la concessione di sovvenzioni, contributi, sussidi ed ausili finanziari e l'attribuzione di vantaggi economici di qualunque genere a persone ed enti pubblici e privati.

19.2
In **AT/ Sovvenzioni, contributi, sussidi, vantaggi economici / Atti di concessione** sono resi pubblici gli atti di concessione di sovvenzioni, contributi, sussidi ed ausili finanziari alle imprese e comunque di vantaggi economici di qualunque genere a persone ed enti pubblici e privati di importo superiore a mille euro. E' altresì aggiornato con cadenza annuale l'elenco dei soggetti beneficiari degli atti di concessione di sovvenzioni, contributi, sussidi ed ausili finanziari alle imprese e di attribuzione di vantaggi economici di qualunque genere a persone ed enti pubblici e privati di importo superiore a mille euro

19.3
La pubblicazione di cui al punto precedente deve avvenire nel rispetto dell'art. 26, c. 4 del D. Lgs 33/2013 che recita *"è esclusa la pubblicazione dei dati identificativi delle persone fisiche destinatarie dei provvedimenti di cui al*

presente articolo, qualora da tali dati sia possibile ricavare informazioni relative allo stato di salute ovvero alla situazione di disagio economico-sociale degli interessati".

Art. 20: Bilanci

20.1
In **AT/ Bilanci / Bilancio preventivo e consuntivo** è reso pubblico il **bilancio di previsione** di ciascun anno in forma sintetica, aggregata e semplificata, anche con il ricorso a rappresentazioni grafiche.

20.2
In **AT/ Bilanci / Bilancio preventivo e consuntivo** è reso pubblico il **bilancio consuntivo** di ciascun anno in forma sintetica, aggregata e semplificata, anche con il ricorso a rappresentazioni grafiche

Art. 21: Beni immobili e gestione patrimonio

21.1
In **AT/ Beni immobili e gestione patrimonio/ Patrimonio immobiliare** sono pubblicate informazioni identificative degli immobili posseduti e detenuti (se presenti).

21.2
In **AT/ Beni immobili e gestione patrimonio/ Canoni di locazione o affitto** sono pubblicate informazioni sui canoni di locazione o di affitto versati o percepiti (se presenti)

Art. 22: Controlli e rilievi sull'amministrazione

22.1
In **AT/ Controlli e rilievi sull'amministrazione/ Organi di revisione amministrativa e contabile** sono pubblicate le relazioni degli organi di revisione amministrativa e contabile al bilancio di previsione o budget, alle relative variazioni e al conto consuntivo o bilancio di esercizio

22.2
In **AT/ Controlli e rilievi sull'amministrazione/ Corte dei conti** sono resi pubblici, ove presenti, i rilievi della Corte dei conti ancorchè non recepiti riguardanti l'organizzazione e l'attività delle amministrazioni stesse e dei loro uffici.

Art. 23: Servizi erogati

23.1
In **AT/ Servizi erogati / Carta dei servizi e standard di qualità** é pubblicata la carta dei servizi o documento contenente gli standard di qualità dei servizi pubblici

Art. 24: Pagamenti dell'amministrazione

24.1
In **AT/ Pagamenti dell'amministrazione / Dati sui pagamenti** é pubblicata una tabella con i dati dei pagamenti trimestrali effettuati (data, mandato, causale, importo, beneficiario)

24.2
In **AT/ Pagamenti dell'amministrazione / Indicatore di tempestività dei pagamenti** é pubblicato l'indicatore trimestrale di tempestività dei pagamenti relativi agli acquisti di beni, servizi, prestazioni professionali e forniture. Con cadenza annuale è anche pubblicato l'indicatore annuale di tempestività dei pagamenti relativo all'anno solare. Anche con cadenza annuale potrà essere pubblicato l'ammontare complessivo dei debiti e il numero delle imprese creditrici.

24.3
In **AT/ Pagamenti dell'amministrazione / IBAN e pagamenti informatici** sono resi noti i codici IBAN del conto di pagamento e modalità di effettuazione di pagamenti anche telematici. In particolare devono essere fornite le informazioni per l'utilizzo di PagoInRete, Piattaforma del MIUR per i pagamenti on-line di tasse, contributi e premi assicurativi a carico dei genitori.

Art. 25: Altri contenuti

25.1
In **AT/ Altri contenuti / Prevenzione della Corruzione** sono pubblicati:

- Il **Piano triennale di prevenzione della corruzione e per la trasparenza** redatto e pubblicato dall'Ufficio Scolastico Regionale competente per tutte le scuole del territorio regionale. Aggiornamento annuale.
- Il nome ed i contatti email e telefonici del **responsabile della prevenzione della corruzione e per la trasparenza**
- Il nome ed i contatti email e telefonici dei **referenti della prevenzione della corruzione e per la trasparenza**
- Il nominativo del **Responsabile Anagrafe per la Stazione Appaltante (RASA)** che ha il compito di tenere aggiornate le informazioni dell'Anagrafe Unica delle Stazioni Appaltanti (AUSA)
- Regolamenti per la prevenzione e la repressione della corruzione e dell'illegalità (laddove adottati)
- Relazione del responsabile della prevenzione della corruzione recante i risultati dell'attività svolta (entro il 15 dicembre di ogni anno).
- Atti adottati in ottemperanza a provvedimenti della ANAC in materia di vigilanza e controllo nell'anticorruzione
- Atti di accertamento delle violazioni delle disposizioni di cui al d.lgs. n. 39/2013
- Il patto di integrità da far firmare alle ditte fornitrici
- Informazioni sulla vigente normativa in materia di segnalazione degli illeciti da parte dei dipendenti e sulle procedure di segnalazione adottate dall'amministrazione

25.2

In **AT/ Altri contenuti / Accesso civico** sono pubblicati:

- Nomi Uffici competenti cui è presentata la richiesta di accesso civico, nonchè modalità per l'esercizio di tale diritto, con indicazione dei recapiti telefonici e delle caselle di posta elettronica istituzionale e nome del titolare del potere sostitutivo, attivabile nei casi di ritardo o mancata risposta, con indicazione dei recapiti telefonici e delle caselle di posta elettronica istituzionale.
- Elenco delle richieste di accesso (civico e generalizzato) con indicazione dell'oggetto e della data della richiesta nonché del relativo esito con la data della decisione. Aggiornamento semestrale.

25.3

In **AT/ Altri contenuti / Privacy** sono pubblicati contatti titolare del trattamento e de Responsabile Protezione Dati (RPD), informative, eventuali moduli di consenso, politica protezione dati personali , modulo per l'esercizio dei diritti in materia di dati personali

25.4

In **AT/ Altri contenuti / Accessibilità e Catalogo dei dati, metadati e banche dati** sono pubblicati:

- Catalogo dei dati, dei metadati definitivi e delle relative banche dati in possesso dell'amministrazione
- Obiettivi di accessibilità dei soggetti disabili agli strumenti informatici per l'anno corrente (entro il 31 marzo di ogni anno)

25.5

In **AT/ Altri contenuti / Dati ulteriori** sono pubblicati dati, informazioni e documenti ulteriori che le pubbliche amministrazioni non hanno l'obbligo di pubblicare ai sensi della normativa vigente e che non sono riconducibili alle sottosezioni indicate. Secondo quanto disposto dall'art. 4, c. 3, del d.lgs. n. 33/2013, nel caso di pubblicazione di dati non previsti da norme di legge si deve procedere alla anonimizzazione dei dati personali eventualmente presenti.

Capo III

Ruoli e responsabilità

Art. 26: Responsabile della trasparenza

26.1

Il responsabile della trasparenza per l'istituzione scolastica è il Direttore Generale dell'Ufficio Scolastico della Regione che svolge stabilmente un'attività di controllo sull'adempimento da parte delle amministrazioni scolastiche di propria competenza degli obblighi di pubblicazione previsti dalla normativa vigente, assicurando la completezza, la chiarezza e l'aggiornamento delle informazioni pubblicate, nonche' segnalando alle Autorita' competenti i casi di mancato o ritardato adempimento degli obblighi di pubblicazione.

26.2

Il Responsabile della trasparenza provvede all'aggiornamento del Programma triennale per la trasparenza e l'integrità.

Art. 27: Responsabile della pubblicazione

27.1
Il responsabile della pubblicazione in Amministrazione Trasparente è il Dirigente Scolastico che, in quanto rappresentante legale dell'istituito scolastico, risponde di qualunque contenuto del sito web istituzionale.

Art. 28: Referente per la trasparenza

28.1
Il referente per la trasparenza nominato dal D.S. ha il compito di

- svolgere ogni utile operazione affinché Amministrazione Trasparente sia costantemente aggiornata con dati e informazioni coi criteri di qualità richiesti
- svolgere attività di controllo e stimolo affinché venga assicurato il raggiungimento degli obiettivi fissati in materia di Anticorruzione e trasparenza (in collaborazione col Responsabile Pubblicazione Dati)
- coordinare le iniziative formative e informative in materia di trasparenza a beneficio del personale e della comunità scolastica nelle sue varie componenti, anche mediante la realizzazione delle c.d. "Giornate della Trasparenza".

Art. 29: Incaricati della pubblicazione

29.1
Il personale che materialmente provvede alla pubblicazione dei documenti e delle informazioni in Amministrazione Trasparente è autorizzato quale incaricato della pubblicazione. Di norma è incaricato della pubblicazione lo stesso dipendente che ha l'incarico di formazione dell'atto medesimo.

29.2
Ciascun incaricato della pubblicazione dovrà occuparsi dei documenti di propria pertinenza secondo quanto stabilito dal piano delle attività redatto dal Direttore dei Servizi Generali ed Amministrativi.

29.3
L'incaricato della redazione del documento destinato alla pubblicazione dovrà accertarsi, nella formazione del documento, del rispetto dei principi di necessità e proporzionalità dei dati personali secondo quanto stabilito dalla vigente normativa sulla Privacy

29.4
L'incaricato della pubblicazione, prima della diffusione del documento in AT, dovrà provvedere a rendere non intelligibili i dati personali non pertinenti o non indispensabili rispetto alle specifiche finalità di trasparenza della pubblicazione.

Capo IV

Disposizioni finali

Art. 30: Violazione degli obblighi di trasparenza – Sanzioni

30.1
L'inadempimento degli obblighi di pubblicazione previsti dal presente regolamento costituisce violazione della normativa in materia di trasparenza (D. Lgs 33/2013) e di lotta alla corruzione (L. 190/2012) e costituisce elemento di valutazione della responsabilità dirigenziale. Contro tali violazioni può ricorrere il cittadino facendo segnalazione al **Responsabile della Prevenzione della Corruzione e per la Trasparenza** dell'istituto o facendo ricorso all'Ufficio del **Difensore Civico Digitale** stabilito presso AGID.

30.2
Il Responsabile della pubblicazione non risponde dell'inadempimento degli obblighi di cui al precedente punto se prova che tale inadempimento è dipeso da causa a esso non imputabile.

Art. 31: Entrata in vigore

31.1
Il presente regolamento entra in vigore contestualmente alla sua pubblicazione.

Quartu Sant'Elena, 03/04/24

Il Dirigente Scolastico
Prof. Massimo Mocci

Documento informatico firmato digitalmente ai sensi del D.Lgs 82/2005 s.m.i. e norme collegate, il quale sostituisce il documento cartaceo e la firma autografa

Liceo Classico Linguistico e Scienze Umane B.R. Motzo

Sede: Via Don Sturzo, 4, 09045 Quartu Sant'Elena (CA)
Telefono: 070/825629 **Sito istituzionale:** liceomotzo.edu.it
E-mail: CAPC09000E@istruzione.it **PEC:** CAPC09000E@pec.istruzione.it
C.U.: UFAGLG **C.F.:** 92168540927

Allegato IV: Disciplinare Interno per l'uso di Internet e della posta elettronica

1. Premessa

L'uso degli strumenti informatici, della posta elettronica e l'accesso ad Internet da parte delle amministrazioni pubbliche si và sempre più diffondendo sotto l'impulso della nuova legislazione, con l'obiettivo di migliorare l'efficienza operativa, contenere i costi ed assicurare una maggiore qualità delle prestazioni.
I servizi informativi sono ormai diventati fondamentali anche per gli istituti scolastici che sempre più dovranno utilizzare strumenti come la posta elettronica ed Internet per fornire servizi all'utenza e per migliorare la propria efficienza.
In particolare, in seguito alle procedure di lavoro agile (c.d. smart working) adottate in seguito alla pandemia di COVID-19, l'utilizzo dei sistemi informatici da remoto tramite sistemi cloud è entrato a far parte delle modalità ordinarie di svolgimento del lavoro da parte dei dipendenti dell'amministrazione.

Pertanto è necessario che siano adottate adeguate ed opportune misure di sicurezza volte a proteggere la disponibilità e l'integrità delle risorse informative e a tutelare la riservatezza dei dati personali di tutti. A questo proposito si richiama quanto viene riportato anche nelle Linee Guida per la Sicurezza ICT delle Pubbliche Amministrazioni del CNIPA (Comitato Nazionale per l'Informatica nella Pubblica Amministrazione):

"Tutti i dipendenti dell'Amministrazione sono tenuti ad utilizzare i servizi di rete solo nell'ambito delle proprie mansioni di lavoro, secondo direttive circostanziate, essendo consapevoli che ogni accesso ad Internet può essere facilmente ricondotto alla persona che lo ha effettuato. Occorre quindi che i dipendenti si comportino con il massimo livello di professionalità quando operano in Internet, evitando eventi dannosi, anche al fine di non danneggiare l'immagine dell' Amministrazione".

Dall'esame di diversi reclami, segnalazioni e quesiti pervenuti, il Garante per la protezione dei dati personali ha preso atto dell'esigenza di prescrivere ai datori di lavoro pubblici e privati alcune misure, necessarie o opportune, per conformare alle vigenti disposizioni in materia di Privacy il trattamento di dati personali effettuato per verificare il corretto utilizzo, nel rapporto di lavoro, della Posta elettronica e di Internet.
A tale scopo è stato emanato il provvedimento generale pubblicato sul Bollettino n. 81 del Marzo 2007 e, successivamente, sulla Gazzetta Ufficiale – Serie generale n. 58 del 10.03.2007 (di seguito "il Provvedimento").
Con il presente disciplinare si fornisce concreto riscontro alle prescrizioni del Garante e si conforma a quanto previsto nelle conclusioni del Provvedimento, al punto 2), lett. a).

2. Principi

Il presente disciplinare viene predisposto nel rispetto della vigente disciplina in materia di Privacy, con riguardo, in particolare, alle norme del Reg. UE 679/2016 (GDPR) e del D. Lgs. 196/03 (Codice in materia di protezione dei dati personali) che disciplinano il trattamento effettuato dai soggetti pubblici.

L'Istituto Scolastico garantisce che il trattamento dei dati personali dei dipendenti relativo all'utilizzo da parte degli stessi di risorse informatiche proprie o dell'amministrazione, si conforma ai seguenti principi:

a) il principio di minimizzazione, secondo cui i sistemi informativi e i programmi informatici devono essere configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi in relazione alle finalità perseguite (art. 3 del Codice; par. 5.2 del Provvedimento);
b) il principio di traspearenza, secondo cui le caratteristiche dei trattamenti devono essere rese note agli interessati poiché le tecnologie dell'informazione, in modo più marcato rispetto ad apparecchiature tradizionali, permettono di svolgere trattamenti ulteriori rispetto a quelli connessi ordinariamente all'attività lavorativa, anche all'insaputa o, comunque, senza la piena consapevolezza dei lavoratori

3. Utenti autorizzati all'uso di Internet

Per quanto riguarda l'uso delle dotazioni informatiche e l'accesso ad internet si individuano 3 tipologie di utenti:

1) Personale amministrativo: autorizzato all'uso per lo svolgimento dell'attività amministrativa
2) Personale docente: autorizzato all'uso per qualunque attività educativa, didattica e formativa.
3) Alunni: autorizzato limitatamente all'attività educativa, didattica e formativa programmata dai docenti

4. Ubicazione postazioni di lavoro

Per quanto riguarda il personale amministrativo, ogni dipendente riceve indicazione della postazione di lavoro a lui assegnata al momento della presa di servizio, ovvero in caso di cambiamento della propria posizione. L'uso di tale postazione non è tuttavia da ritenersi esclusivo e ciascun dipendente a seconda delle necessità potrà operare su altro PC non direttamente assegnato ***usando sempre la propria credenziale di accesso personale*** (nome utente e password).

L'accesso ad Internet da parte del personale tecnico, docente e degli alunni potrà avvenire nelle classi, nei laboratori ed in qualunque altro luogo a tale attività destinato.

5. Sistema di autenticazione

Al fine di ridurre al minimo il rischio di impieghi abusivi, l'accesso alle postazioni destinate all'attività amministrativa è protetto tramite sistema di autenticazione che richiede l'immissione di un apposito codice utente e della relativa password. La gestione degli utenti è fatta in maniera centralizzata sul server di segreteria su cui è configurato un dominio in ambiente Windows server e nel quale potranno quindi essere conservate informazioni relative agli accessi dei singoli utenti.

6. Istruzione e formazione del personale

Il personale ha ricevuto specifiche istruzioni scritte in merito al comportamento da adottare nell'uso delle dotazioni informatiche messe a loro disposizione. In base alla criticità dei trattamenti effettuati da ciascuna componente, sono stati approntati specifici interventi di formazione.

7. Misure di tipo tecnologico connesse all'uso della posta elettronica

Ai fini dell'utilizzo corretto delle caselle di posta elettronica personali messe a disposizione del personale e degli alunni da parte dell'amministrazione, si mettono in evidenza i seguenti punti:

- *E' consentito l'utilizzo del proprio account a fini privati e personali, purché tale utilizzo non sia causa, diretta o indiretta di disservizi dei sistemi elaborativi e dei servizi di posta elettronica dell'Amministrazione.*
- *Gli utenti del servizio di posta elettronica sono tenuti ad usarlo in modo responsabile, cioè, rispettando le leggi, la presente e altre politiche e procedure della Scuola e del Ministero della Pubblica Istruzione e secondo normali standard di cortesia, correttezza, buona fede e diligenza professionale*
- *E' fatto divieto a tutti gli utenti di utilizzare il servizio di posta elettronica per inviare messaggi dannosi, di tipo offensivo o sconveniente, come ad esempio, a titolo non esaustivo, messaggi che riportino contenuti o commenti oltraggiosi su argomenti sessuali, razziali, religiosi, politici, ecc. e comunque ogni altra tipologia di messaggio che possa arrecare danno alla reputazione della Scuola o del Ministero della Pubblica Istruzione.*
- *E' vietato l'uso del servizio di posta elettronica a scopi commerciali o di profitto personale e per attività illegali.*
- *L'Amministrazione registra e conserva, in forma anonima, i dati delle caselle di posta elettronica messe a disposizione dei propri utenti, tramite scrittura in appositi file di log, delle seguenti informazioni minime: mittente del messaggio; destinatario/i; giorno ed ora dell'invio; esito dell'invio. L'amministrazione, inoltre, potrà procedere alla cancellazione dell'account qualora l'esistenza dello stesso non sia più compatibile con le condizioni e le finalità per cui era stato originariamente attivato (ad es. il dipendente non è più in servizio, l'alunno termina la propria permanenza nell'istituto).*

Per evitare ogni interferenza con la sfera privata del personale docente e ATA, qualunque comunicazione di interesse amministrativo o di lavoro dovrà avvenire per mezzo delle caselle istituzionali.

La consultazione della posta elettronica da parte dei dipendenti può quindi riguardare:

- caselle personali
- caselle istituzionali di lavoro

UTILIZZO DELLE CASELLE PERSONALI

Il personale può consultare in orario di servizio caselle personali per motivi legati alla propria attività lavorativa. La gestione deve essere effettuata tramite servizi di "webmail": non è consentito configurare su computer dell'Istituto appositi programmi tipo Outlook o Thunderbird per gestire le proprie caselle personali (anche per garantire al dipendente la dovuta riservatezza).

Nell'uso di caselle personali all'interno della scuola, al dipendente non è comunque consentito:

- inviare messaggi dannosi, di tipo offensivo o sconveniente, come ad esempio, a titolo non esaustivo, messaggi che riportino contenuti o commenti oltraggiosi su argomenti sessuali, razziali, religiosi, politici, ecc. e comunque ogni altra tipologia di messaggio che possa arrecare danno alla reputazione della Scuola o del MIUR;
- l'uso del servizio di posta elettronica a scopi commerciali o di profitto personale e per attività illegali;
- utilizzare tecniche di "mail spamming" cioè di invio massiccio di comunicazioni a liste di distribuzione extra lavorative o azioni equivalenti.

UTILIZZO DELLE CASELLE ISTITUZIONALI DI LAVORO

Le caselle istituzionali sono gestite dagli incaricati in base ai compiti loro assegnati. In caso di assenza dell'incaricato abituale, questo potrà essere sostituito da altro personale, in base

all'organizzazione interna del lavoro disposta da D.S. o D.S.G.A.: quindi tali caselle devono essere utilizzate solo a scopo lavorativo e NON devono essere utilizzate come caselle personali.
Oltre alle disposizioni impartite per l'utilizzo delle caselle personali, si aggiungono le seguenti disposizioni:

- Evitare di aprire messaggi provenienti da mittenti sconosciuti e che contengono allegati sospetti (file con estensione .exe, .scr, .pif, .bat, .cmd,....). In caso di dubbio consultare un tecnico.
- Nel caso in cui si debba inviare un documento all'esterno dell'Istituto, se non specificamente destinato alla modifica, è preferibile utilizzare il formato *.pdf.
- Evitare che la diffusione incontrollata di "Catene di Sant'Antonio" (messaggi a diffusione capillare e moltiplicata) limiti l'efficienza del sistema di posta.
- Evitare di inviare allegati di dimensioni eccessive (se necessario usare formati compressi come *.zip, *.rar,...)
- L'iscrizione a "mailing list" esterne è concessa solo per motivi professionali, prima di iscriversi occorre verificare in anticipo se il sito è affidabile. In caso di dubbio, è necessario contattare preventivamente il DS, il DSGA o un suo delegato, che definiranno l'effettiva sicurezza della stessa, consultandosi, se necessario, con l'amministratore di sistema e/o l'RPD dell'istituto.
- La casella di posta deve essere mantenuta in ordine.

8. Misure di tipo tecnologico connesse all'uso di Internet

L'Istituto Scolastico intende limitare nel maggior grado possibile i controlli sulla navigazione (che potrebbero determinare il trattamento di informazioni personali o sensibili anche non pertinenti l'amministrazione).
Per tale motivo è fondamentale il rispetto delle disposizioni elencate, che hanno il fine di ridurre il rischio di usi impropri della "navigazione".

1. Al personale non è consentito, durante le ore di lavoro:
   - servirsi o dar modo ad altri di servirsi della stazione di accesso a internet per attività non istituzionali, per attività poste in essere in violazione del diritto d'autore o altri diritti tutelati dalla normativa vigente;
   - utilizzare sistemi Peer to Peer (P2P), di file sharing, podcasting, webcasting social network o similari (salvo specifiche attività espressamente autorizzate per le finalità istituzionali).
   - Utilizzare sistemi Social Network quali twitter, facebook, etc., salvo specifiche attività espressamente autorizzate per le finalità istituzionali.
2. Ogni utente deve tenere comportamenti tali da ridurre il rischio di attacco al sistema informatico mediante virus o mediante ogni altro software aggressivo (attenzione nell'aprire mail e relativi allegati, non navigare su siti poco professionali, ecc..)
3. Ogni utente è tenuto a controllare la presenza e il regolare funzionamento del software antivirus, segnalando ogni eventuale problema all'amministratore di sistema.

Si ricorda poi che scaricare file audio e video (o comunque grandi quantità di dati) è in grado di degradare le prestazioni offerte dal servizio agli altri utenti: per tale motivo ciò può avvenire solo se necessario e, possibilmente, al di fuori dei momenti "di punta" a livello di Istituto.

Per garantire la sicurezza informatica ed il controllo del corretto utilizzo dell'accesso ad Internet l'istituto si è dotato di strumenti specifici che consentono:

- La protezione da accessi non autorizzati provenienti da Internet
- Controlli antivirus centralizzati

- configurazione di filtri che prevengono determinate operazioni non correlate all'attività lavorativa (quali a titolo esemplificativo e non esaustivo: l'accesso ai siti inseriti in black list individuati dall'Istituto, il download di file o software aventi particolari caratteristiche dimensionali o di tipologia di dato), anche in modo differenziato per le diverse postazioni o tipologie di accesso;
- la determinazione di informazioni sulla navigazione Internet che consentono la conservazione di informazioni relative ad utente, PC, ora di accesso, pagine accedute, etc.

Si precisa che ulteriori tracce dell'operato di ciascun utente, lasciate sui PC, sui server e sui programmi impiegati, potranno essere utilizzate per l'individuazione e la sanzione di eventuali comportamenti anomali.
La conservazione nel tempo dei dati relativi all'uso degli strumenti informatici verrà fatta per il periodo strettamente limitato al perseguimento di finalità organizzative, produttive e di sicurezza ovvero in adempimento di obblighi previsti dalla legge;

9. Disposizioni per il lavoro da remoto (telelavoro)

Il personale che svolge la propria attività in modalità di lavoro agile deve attenersi alle raccomandazioni elaborate da Cert-PA di AgID per il rispetto delle misure minime di sicurezza informatica per le pubbliche amministrazioni fissate dalla circolare 17 marzo 2017, n. 1 che devono essere garantite anche dal personale che svolge la propria attività lavorativa da remoto e riportate di seguito:

1. segui prioritariamente le policy e le raccomandazioni dettate dalla tua Amministrazione;
2. utilizza i sistemi operativi per i quali attualmente è garantito il supporto (non utilizzare, ad esempio, macchine con sistema operativo windows XP o windows 7 di cui Microsoft ha terminato il supporto);
3. effettua costantemente gli aggiornamenti di sicurezza del tuo sistema operativo;
4. assicurati che i software di protezione del tuo sistema operativo (Firewall, Antivirus, ecc.) siano abilitati e costantemente aggiornati;
5. assicurati che gli accessi al sistema operativo siano protetti da una password sicura di almeno 8 caratteri contenente almeno una lettera maiuscola, un numero ed un carattere speciale;
6. non installare software proveniente da fonti/repository non ufficiali;
7. blocca l'accesso al sistema e/o configura la modalità di blocco automatico quando ti allontani dalla postazione di lavoro;
8. non cliccare su link o allegati contenuti in email sospette;
9. utilizza l'accesso a connessioni Wi-Fi adeguatamente protette;
10. collegati a dispositivi mobili (pen-drive, hdd-esterno, etc) di cui conosci la provenienza (nuovi, già utilizzati, forniti dalla tua Amministrazione);
11. effettua sempre il log-out dai servizi/portali utilizzati dopo che hai concluso la tua sessione lavorativa.

Si coglie l'occasione per dare le seguenti ulteriori disposizioni:

- Utilizza esclusivamente servizi cloud certificati dall'amministrazione (tramite nomina a responsabile del trattamento) per il trattamento dei dati personali di cui l'amministrazione è titolare;
- nel caso in cui utilizzi un PC personale per svolgere l'attività lavorativa, prima del suo primo utilizzo, installa un buon antivirus e fai una accurata scansione preventiva per rimuovere qualunque software malevolo;

- non memorizzare sui dispositivi le password di accesso alle piattaforme ed ai sistemi utilizzati per il lavoro a distanza;
- non memorizzare sul client di posta elettronica le credenziali di accesso alle caselle istituzionali;
- accertati di aver impostato una password sicura sul router utilizzato per l'accesso ad Internet (accertati di non aver lasciato la password di default proposta dal costruttore e nota a qualunque malintenzionato);
- se utilizzi una connessione wi-fi, accertati di adottare una password sicura per il suo accesso (mai lasciare accessi liberi alla rete wi-fi).

10. Trattamenti esclusi

L'Istituto Scolastico non effettua controlli prolungati, costanti o indiscriminati dell'uso di Internet e Posta elettronica da parte dei dipendenti.
L'Istituto Scolastico non effettua trattamenti di dati personali mediante sistemi hardware e software che mirano al controllo a distanza di lavoratori attraverso:

- lettura e registrazione sistematica dei messaggi di posta elettronica personali dei dipendenti o dei relativi dati esteriori;
- riproduzione ed eventuale memorizzazione sistematica delle pagine web visualizzate dal lavoratore;
- lettura e registrazione dei caratteri inseriti dai lavoratori tramite la tastiera ovvero dispositivi analoghi a quello descritto;

11. Gradualità dei controlli

1. Nel caso in cui un evento dannoso o una situazione di pericolo non sia stato impedito con preventivi accorgimenti tecnici, il Dirigente Scolastico può adottare eventuali misure che consentano la verifica di comportamenti anomali.
2. Per quanto possibile, sarà preferito un controllo preliminare su dati aggregati, riferiti all'intera struttura lavorativa o a sue aree. Il controllo anonimo può concludersi con un avviso generalizzato relativo ad un rilevato utilizzo anomalo degli strumenti d'Istituto e con l'invito ad attenersi scrupolosamente a compiti assegnati e istruzioni impartite. L'avviso può essere circoscritto a dipendenti afferenti all'area o settore in cui è stata rilevata l'anomalia.
3. La presenza di successive anomalie potrà comportare controlli su base individuale.
4. La rilevazione delle anomalie e delle verifiche tecniche è a cura dell'Amministratore di Sistema che potrà anche intervenire su richiesta del Dirigente Scolastico per la verifica di situazioni anomale o sospette.
5. Responsabile dei successivi e consequenziali provvedimenti è il Dirigente Scolastico.

12. Sanzioni

1. È fatto obbligo a tutti i Lavoratori di osservare le disposizioni del presente disciplinare e qualunque altra comunicata dall'Amministrazione in materia di sicurezza e gestione delle attrezzature informatiche.
2. Il mancato rispetto o la violazione delle regole contenute nel presente Disciplinare è perseguibile con tutte le azioni civili e penali previste dalla legge, nonché con i provvedimenti disciplinari, in conformità a quanto previsto dalle disposizioni normative e contrattuali vigenti per il personale o per l'area dirigenza del comparto Regioni ed Autonomie Locali. Rimane ferma ogni ulteriore forma di responsabilità civile e penale, quali ad es.:
   - Violazioni di dati personali e della tutela dell'immagine;

- diffamazione;
- accesso abusivo ad un sistema informatico e telematico;
- violazione della legge sul copyright.

3. Il codice di comportamento ed il codice disciplinare sono consultabili nel sito internet dell'Ente

13. Disposizioni ulteriori

1. I dati personali inerenti i Lavoratori non possono essere portati a conoscenza di terzi non autorizzati. I colleghi di lavoro della persona interessata sono considerati terzi.
2. L'Amministrazione, nell'ambito di procedimenti disciplinari e/o di procedimenti penali di cui all'art. 11 del presente Disciplinare e nel rispetto del principio di protezione dei dati personali e del divieto di controllo a distanza del Lavoratore, procede alla conservazione delle "registrazioni a giornale" (log file) relative all'utilizzazione di Internet e/o della Posta Elettronica e/o dei files delle telefonate e/o dei Fax e dei Fax mail, fino alla conclusione dei relativi procedimenti.
3. Il presente documento viene portato a conoscenza di tutti i Lavoratori, indicati all'art. 1 del presente Disciplinare, mediante pubblicazione nei sito internet.

14. Aggiornamento periodico

Il presente regolamento è aggiornato con cadenza almeno annuale o in caso di rinvenimento di soluzioni tecnologiche ritenute più idonee a tutelare i dati personali dei lavoratori, e portato a conoscenza di tutti i lavoratori mediante affissione all'albo dell'istituto e pubblicazione nell'intranet istituzionale.

Quartu Sant'Elena, 03/04/24

Il Dirigente Scolastico
Prof. Massimo Mocci