Regolamento disciplinante ruoli e responsabilità in merito alla protezione e libera circolazione dei dati personali ai sensi del Regolamento Generale Protezione Dati (UE) 2016/679

TITOLARE DEL TRATTAMENTO:	**Polo scolastico 2 – Liceo scientifico "Torelli" – Fano e Pergola (PU)**
Sede centrale:	Fano – Viale Kennedy N. 30
Tel.:	0721 - 800809
PEC:	psps01000g@pec.istruzione.it

Versione/Revisione:	1.0
Data di revisione:	25/10/2022
Redatto da:	Team DPO – Morolabs Srl
Approvato da:	Consiglio di Istituto
Livello di Riservatezza:	Riservato

Sommario

CAPO I - DISPOSIZIONI GENERALI

Art. 1. - Oggetto

1. Il presente Regolamento ha per oggetto la protezione dei diritti e delle libertà delle persone fisiche in ordine al trattamento dei dati personali effettuato dal titolare nonché misure procedimentali e regole di dettaglio, nel rispetto di quanto previsto dal Regolamento europeo (General Data Protection Regulation del 27 aprile 2016 n. 679, di seguito indicato con "GDPR", Regolamento Generale Protezione Dati), dal Codice in materia di dati personali (D.Lgs. n. 196/2003 s.m.i.) aggiornato dal D.Lgs. n. 101/2018, dalle Linee guida e raccomandazioni del Garante e dalle Dichiarazioni del gruppo di lavoro articolo 29 sulla protezione dei dati (WP29) – 14/EN.
2. Il presente Regolamento individua i soggetti mediante i quali il **Polo scolastico 2 – Liceo scientifico "Torelli" – Fano e Pergola (PU)** esercita le funzioni di titolare del trattamento dei dati personali, i loro ruoli e responsabilità.

Art. 2. - Definizioni

1. Il presente regolamento si avvale delle seguenti definizioni:
   - Per "***Codice***", il Codice in materia di protezione dei dati personali introdotto con il decreto legislativo 30 giugno 2003, n. 196, modificato e integrato con il Decreto Legislativo 101/2018 recante "Disposizioni per l'adeguamento della normativa nazionale alle Disposizioni del Regolamento UE 2016/679;
   - per ***"Regolamento"*** *il "Regolamento UE 2016/679* 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" (GDPR);
   - per *"**trattamento**"*, qualunque operazione o complesso di operazioni, svolti con l'ausilio dei mezzi elettronici o comunque automatizzati, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distribuzione di dati personali;
   - per *"**dato personale**",* qualunque informazione relativa a persona fisica, identificata o identificabile anche indirettamente e rilevata con trattamenti di immagini effettuati mediante gli impianti di videosorveglianza;
   - per ***"titolare del trattamento dei dati personali"*** *o anche "**titolare",*** **l'Istituto Polo scolastico 2 – Liceo scientifico statale "Torelli" di Fano e Pergola (PU),** cui competono le decisioni in ordine alle finalità ed alle modalità del trattamento dei dati personali. Al titolare, anche unitamente ad altro titolare, spettano le decisioni in ordine alle modalità del trattamento e agli strumenti utilizzati. Tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, il titolare del trattamento mette in atto misure tecniche e organizzative adeguate a garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente alla normativa in materia di protezione dei dati personali.
   - per ***"responsabile del trattamento dei dati personali"*** *o anche "**responsabile"***, la persona fisica o giuridica, individuata dal Titolare, a cui viene esternalizzata un'attività o un servizio che richiede connesse operazioni di trattamento di dati personali per conto del Titolare. I trattamenti da parte di un responsabile del trattamento sono disciplinati da un contratto o da altro atto giuridico a norma del diritto dell'Unione europea o degli Stati membri.
   - per ***"responsabile della protezione dei dati" o "RPD" o "D.P.O"*** si intende il soggetto esterno con competenze giuridiche, informatiche e di analisi dei processi, nominato dal titolare del trattamento, che affianca il medesimo nella valutazione e gestione del trattamento dei dati nel rispetto delle normative sulla privacy, vigilando sull'osservanza delle normative stesse;

- per **"*autorizzati*"**, chiunque, sia esso definito "designato" o "incaricato", agisce sotto l'autorità del titolare o del responsabile che abbia accesso e gestisca dati personali per le funzioni che gli competono;
- per **"*designati*"**, coloro che operano sotto l'autorità del titolare e sono stati individuati da questi a svolgere specifici compiti e funzioni di primo livello connessi al trattamento di dati personali;
- per **"*incaricati*"**, coloro che operano sotto l'autorità del titolare e svolgono compiti di secondo livello in merito al trattamento dei dati personali;
- per **"*amministratore di sistema*"**, si intende il personale sistemistico e di networking, che ha facoltà di accesso alle informazioni anche senza i vincoli e le protezioni del livello applicativo;
- per **"*interessato*"**, la persona fisica a cui si riferiscono i dati personali;
- per "***dato personale comune***": qualsiasi informazione riguardante una persona fisica(interessato), identificata o identificabile. 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 di caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.
- per "***dati personali particolari***": I dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, (già dati sensibili) nonché i 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.
- per "***dati giudiziari***": i dati personali idonei a rivelare condanne penali, reati o connesse misure di sicurezza, oltre che i provvedimenti di cui all'articolo 3, comma 1, lettere da a) a o) e da r) a u), del D.P.R. 14 novembre 2002, n. 313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale.
- per ***"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 e 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.
- per ***"pseudonimizzazione"***: il trattamento di 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.
- per ***"Garante"***: l'autorità pubblica di controllo indipendente di cui agli artt. 2-bis e 153 e ss. Del Codice, istituita dalla legge 31 dicembre 1996, n. 675, per vigilare sulla corretta applicazione della normativa in materia di protezione dei dati personali.

Art. 3. - Finalità del trattamento

2. Il Titolare garantisce che il trattamento dei dati personali, a tutela delle persone fisiche, si svolge nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, all'integrità, alla disponibilità delle informazioni personali e dell'identità personale a prescindere dalla loro nazionalità o della loro residenza.
3. Il Titolare, nell'ambito delle sue attribuzioni, 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.

4. Ai fini della tutela dei diritti e delle libertà delle persone fisiche in ordine al trattamento dei dati personali, tutti i processi di competenza del Titolare sono gestiti conformemente alle disposizioni del Codice, del GDPR e del presente Regolamento.

Art. 4. - Principi e responsabilizzazione

1. Vengono integralmente recepiti, nell'ordinamento interno del titolare, i principi del GDPR, per effetto dei quali 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, 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").
2. Il titolare è competente per il rispetto dei principi sopra declinati, ed è in grado di comprovarlo in base al principio di "responsabilizzazione".

Art. 5. - Liceità del trattamento dei dati personali comuni

1. Vengono integralmente recepiti, nell'ordinamento interno del titolare, le disposizioni del GDPR in odine alla liceità del trattamento dei dati personali comuni 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.

Art. 6. - Liceità del trattamento dei dati personali particolari

1. Il Titolare si conforma a quanto previsto dall'art. 9 GDPR che disciplina il trattamento di categorie particolari di dati personali. Nello specifico il GDPR sancisce il divieto di 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. Nel paragrafo successivo l'art. 9 GPDR individua le circostanze in cui tale divieto non si applica:

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 riguarda dati personali resi manifestamente pubblici dall'interessato;

e) il trattamento è necessario per accertare, esercitare o difendere un diritto in sede giudiziaria o ogniqualvolta le autorità giurisdizionali esercitino le loro funzioni giurisdizionali;

Art. 7. - Condizioni per il consenso

1. Qualora il trattamento sia basato sul consenso, il Titolare del trattamento deve essere in grado di dimostrare che l'interessato ha prestato il proprio consenso al trattamento dei propri dati personali. Se il consenso dell'interessato è prestato nel contesto di una dichiarazione scritta che riguarda anche altre questioni, la richiesta di consenso è presentata in modo chiaramente distinguibile dalle altre materie, in forma comprensibile e facilmente accessibile, utilizzando un linguaggio semplice e chiaro. Nessuna parte di una tale dichiarazione che costituisca una violazione del presente regolamento è vincolante.
2. L'interessato ha il diritto di revocare il proprio consenso in qualsiasi momento. La revoca del consenso non pregiudica la liceità del trattamento basata sul consenso prima della revoca. Prima di esprimere il proprio consenso, l'interessato è informato di ciò. Il consenso è revocato con la stessa facilità con cui è accordato.

Art. 8. - Informativa

1. Il titolare, al momento della raccolta dei dati personali, è tenuto a fornire all'interessato, anche avvalendosi del personale incaricato, apposita informativa secondo le modalità previste dagli artt. 13 e 14 del GDPR, in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro, in particolare nel caso di informazioni destinate specificamente ai minori.
2. 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.
3. L'informativa è fornita, mediante idonei strumenti:
   a) 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;
   b) 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 apposita pubblicazione sulla sezione dedicata del sito istituzionale;
   c) 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;
   d) resa in sede di pubblicazione dei bandi, avvisi, lettere d'invito, con l'indicazione dell'incaricato del trattamento dei dati relativi alle procedure, anche tramite diciture brevi richiamanti informative più ampie.
4. 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.
5. L'informativa contiene il seguente contenuto minimo:
   a) l'identità e i dati di contatto del titolare e, ove presente, del suo rappresentante;
   b) i dati di contatto del RPD/D.P.O. ove esistente;
   c) le finalità del trattamento;
   d) i destinatari dei dati;
   e) la base giuridica del trattamento;
   f) l'interesse legittimo del titolare se quest'ultimo costituisce la base giuridica del trattamento;
   g) se il titolare trasferisce i dati personali in Paesi terzi e, in caso affermativo, attraverso quali strumenti;
   h) il periodo di conservazione dei dati o i criteri seguiti per stabilire tale periodo di conservazione;
   i) 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;
   j) il diritto di presentare un reclamo all'autorità di controllo;
   k) 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.
6. Nel caso di dati personali non raccolti direttamente presso l'interessato:

a) il titolare deve informare l'interessato anche 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.

7. 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.
8. 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.

9. 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. È prevista la possibilità di fornire informative "brevi" che richiamino informative più estese.

Art. 9. - Sensibilizzazione e formazione

1. 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 protezione dei dati, e migliorare la qualità del servizio.
2. A tale riguardo, Il titolare organizza, nell'ambito della formazione continua e obbligatoria del personale, specifici interventi di formazione e di aggiornamento, con cadenza almeno annuale, anche eventualmente 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.
3. La partecipazione dei dipendenti agli interventi formativi viene considerata quale elemento di misurazione dell'accountability dell'Istituto.

Art. 10. - Trattamento dei dati del personale

1. Il Titolare tratta i dati, anche di natura sensibile o giudiziaria, dei propri dipendenti per le finalità, considerate di rilevante interesse pubblico, di instaurazione e di gestione di rapporti di lavoro di qualunque tipo, nel rispetto degli obblighi di legge.
2. 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.
3. 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.

4. 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.
5. Il Titolare, nel trattamento dei dati sensibili relativi alla salute dei propri dipendenti, deve rispettare i principi di necessità e indispensabilità.
6. 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.

CAPO II - DIRITTI DEGLI INTERESSATI

Art. 11. - Pubblicità e diffusione di dati personali contenuti in atti e provvedimenti amministrativi

1. Il Titolare, in sede di pubblicazione e diffusione, tramite l'albo pretorio informatico e la rete civica, di dati personali contenuti in atti e provvedimenti amministrativi, assicura, mediante l'implementazione delle necessarie misure tecniche ed organizzative, il rispetto dei seguenti principi:
    a) sicurezza
    b) completezza
    c) esattezza
    d) accessibilità
    e) minimizzazione
    f) legittimità e conformità ai principi di pertinenza, non eccedenza, temporaneità ed indispensabilità rispetto alle finalità perseguite.
2. Laddove documenti, dati e informazioni, oggetto di pubblicazione obbligatoria per finalità di trasparenza, contengano dati personali, questi ultimi devono essere oscurati o pseudonimizzati, tranne deroghe previste da specifiche disposizioni.
3. Salva diversa disposizione di legge, il titolare garantisce la riservatezza dei dati sensibili in sede di pubblicazione all'Albo on line o sulla rete civica, mediante la non identificabilità dei soggetti cui tali dati si riferiscono, adottando gli opportuni accorgimenti in sede di predisposizione degli atti stessi e dei relativi allegati. A tal fine, il titolare adotta e implementa adeguate misure organizzative, di gestione documentale e di formazione.
4. Il titolare si conforma alle Linee guida del Garante in materia di pubblicazione e diffusione di dati personali contenuti in atti e provvedimenti amministrativi.

Art. 12. - Diritto di accesso alla documentazione, diritto di accesso civico e protezione dei dati personali

1. 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.
2. Le attività finalizzate all'applicazione di tale disciplina si considerano di rilevante interesse pubblico.
3. 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.

Art. 13. - Diritti dell'interessato

1. Il Titolare deve garantire ed agevolare, nel rispetto della normativa vigente, l'esercizio dei diritti da parte dell'interessato, adottando ogni misura (tecnica e organizzativa) a ciò idonea.
2. Il Titolare si impegna a non utilizzare i dati che, a seguito di verifiche, dovessero risultare eccedenti o non pertinenti o non necessari. Per garantire un trattamento di dati corretto e trasparente, l'Interessato ha diritto di chiedere, nei limiti degli artt. al Titolare di:
   - accedere ai propri dati e conoscere chi vi ha avuto accesso (art. 15 GDPR);
   - richiedere l'aggiornamento, la rettifica o l'integrazione dei dati (art. 16 GDPR);
   - richiedere la cancellazione («diritto all'oblio») e la limitazione del trattamento se trattati in difformità dalla legge, fatti salvi gli obblighi legali di conservazione (artt. 17 e 18 GDPR);
   - ricevere, nei casi normativamente previsti, in formato strutturato, di uso comune e leggibile da dispositivo automatico i dati personali che lo riguardano forniti ad un Titolare del trattamento unitamente al diritto di trasmettere (se possibile) tali dati ad un altro Titolare, senza impedimenti da parte del Titolare del trattamento cui li ha forniti, qualora:
     - il trattamento si basi sul consenso ai sensi dell'art. 6 GDPR, o dell'art. 9 GDPR o su un contratto ai sensi dell'art. 6 GDPR;
     - il trattamento sia effettuato con mezzi automatizzati (art.20 GDPR);
3. Il presente Regolamento tiene conto della circostanza che, in forza della disciplina del GDPR, 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.
   - opporsi, per motivi legittimi, al trattamento dei dati (art. 21 GDPR).
4. Ai sensi dell'art. 77 GDPR, resta impregiudicato per l'Interessato il suo diritto, qualora ne ricorrano le condizioni, di rivolgere reclamo al Garante per la Protezione dei Dati Personali secondo le modalità indicate sul sito www.garanteprivacy.it .
5. Ogni diritto deve essere valutato anche nel rispetto dei limiti indicati dagli artt. 23 GDPR, 2-undecies e 2-duodecies Codice Privacy.
6. La procedura per esercitare i diritti in materia di protezione dei dati è pubblicata sul sito istituzionale, nell'apposita sezione oppure presso gli uffici.

Art. 14. - Modalità di esercizio dei diritti dell'interessato

1. Per l'esercizio dei diritti dell'interessato, in ordine all'accesso ed al trattamento dei suoi dati personali, si applicano le disposizioni del GDPR, del Codice, del presente Regolamento e della relativa procedura, di seguito descritta.
2. 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.

3. L'interessato può presentare o inviare la richiesta di esercizio dei diritti:
   - al titolare, che conserva e gestisce i dati personali dell'interessato;
   - all'ufficio protocollo generale del titolare o all'ufficio per le relazioni con il pubblico;
   - all'indirizzo mail presente sul sito Istituzionale nella sezione dedicata alla privacy.
4. I soggetti competenti alla valutazione dell'istanza sono:
   - il Dirigente Scolastico;
   - il Responsabile per la protezione dei dati (RPD);

che decidono sull'ammissibilità della richiesta d'accesso e sulle modalità di accesso ai dati.

5. 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.
6. Il titolare si conforma alle Linee guida del Garante in tema di esercizio dei diritti dell'interessato.

Art. 15. - Indagini difensive

1. 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.
2. 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.
3. Il titolare si conforma alle Linee guida del Garante in tema di indagini difensive.

CAPO III – SOGGETTI

Art. 16. - Titolare del trattamento

1. L'Istituto, nella persona del Dirigente Scolastico, è il Titolare del trattamento dei dati personali raccolti o meno in banche dati, automatizzate o cartacee (di seguito indicato con "Titolare").
2. Il Titolare nomina il Responsabile della protezione dei dati (di seguito RPD) tra i soggetti in possesso dei requisiti previsti dal GDPR e stabilisce la durata dell'incarico. Della nomina dà comunicazione al Garante per la Protezione dei Dati Personali e alle strutture interessate.
3. In conformità all'assetto organizzativo del Titolare, ciascuno per il rispettivo ambito di competenza, sono qualificabili come autorizzati al trattamento e distinguibili in due categorie:
   a) Soggetti *Designati* al trattamento (Direttore dei servizi generali e amministrativi "D.S.G.A.")
   b) Soggetti *Incaricati* al trattamento (tutti gli altri dipendenti).

4. I soggetti di cui sopra sono responsabili del rispetto dei principi applicabili al trattamento dei dati personali stabiliti dall'art. 5 GDPR: liceità, correttezza, trasparenza, limitazione della finalità, minimizzazione, esattezza, limitazione della conservazione, integrità e riservatezza, responsabilizzazione.
5. Inoltre, gli stessi soggetti sono tenuti a porre in essere, in funzione del ruolo ricoperto misure tecniche ed organizzative adeguate a garantire, ed essere in grado di dimostrare, che il trattamento di dati personali è effettuato in modo conforme al GDPR.
6. Le misure sono definite e messe in atto per applicare in modo efficace i principi di protezione dei dati e per agevolare l'esercizio dei diritti dell'interessato stabiliti dagli articoli 15-22 GDPR, nonché le comunicazioni e le informazioni occorrenti per il loro esercizio.
7. Al Dirigente Scolastico sono altresì affidati i seguenti compiti:
   a) definire modalità, mezzi di trattamento e rispettive responsabilità in merito all'osservanza degli obblighi previsti in caso di esercizio associato di funzioni e servizi, nonché per i compiti la cui gestione è affidata al Titolare da enti ed organismi statali o regionali, mediante accordo che disciplina la contitolarità ai sensi dell'art. 26 del GDPR;
   b) designare gli autorizzati al trattamento dei dati personali fornendo adeguate istruzioni per il loro corretto trattamento;
   c) nominare e istruire quale Responsabile del trattamento i soggetti pubblici o privati affidatari di attività e servizi per conto dell'Istituto, relativamente alle banche dati gestite da soggetti esterni al Titolare in virtù di convenzioni, di contratti, o di incarichi professionali o altri strumenti giuridici consentiti dalla legge, per la realizzazione di attività connesse alle attività istituzionali;
   d) notificare al Garante della protezione dei dati personali, le violazioni dei dati personali (data breach) e provvedere alla comunicazione della violazione agli interessati, ai sensi degli articoli 33 e 34 del GDPR, secondo quanto disposto all'art. 9, e darne informativa al RPD;
   e) effettuare l'analisi del rischio e la valutazione di impatto del trattamento sulla protezione dei dati personali (di seguito indicata con "DPIA") di cui all'art. 35 del GDPR, nel caso in cui un tipo di trattamento, specie se prevede in particolare l'uso di nuove tecnologie, possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche, tenuto conto di quanto indicato dal successivo art. 10;
   f) adottare misure appropriate per fornire all'interessato le informazioni indicate dall'art. 13 GDPR, qualora i dati personali siano raccolti presso lo stesso interessato o dell'art. 14 GDPR, qualora i dati personali non sono stati ottenuti presso lo stesso interessato, verificando la corretta predisposizione delle informative e curandone il costante aggiornamento, al fine di garantire l'esercizio dei diritti previsti agli artt. da 15 a 18 e da 20 a 22 del GDPR.

Art. 17. - Soggetti autorizzati al trattamento

1. Il GDPR non prevede particolari formalità per l'individuazione dei soggetti che trattano i dati all'interno di un'organizzazione ma richiede (in ossequio al principio dell'accountability) una tracciabilità delle autorizzazioni al trattamento. In tal senso il GDPR fa riferimento in più punti al "*personale che ha accesso permanente o regolare ai dati personali*", o a *"le persone autorizzate al trattamento dei dati personali*".
2. Il nuovo Codice della Privacy prevede che sia il titolare a individuare le modalità più opportune per autorizzare al trattamento dei dati personali le persone che effettuano operazioni di trattamento sotto la propria autorità (art. 2-quaterdecies CP).
3. A tal fine, con il presente Regolamento, si individuano diversi livelli di autorizzazione funzionale, coerentemente con l'organigramma dell'Ente e, in linea generale, si prevede che le autorizzazioni, ex 2-quaterdecies CP, a trattare i dati personali sono connesse alle autorizzazioni relative ai profili informatici assegnati ai vari dipendenti.

4. Si specifica che, sotto il profilo del trattamento dei dati personali**, i soggetti autorizzati si suddividono in:**

   A. **DESIGNATI** (responsabili della conformità)

   Con il presente Regolamento si individua quale designato al trattamento dei dati (o responsabili della conformità), in ragione e nei limiti del loro mandato, la seguente figura:

   - Il D.S.G.A., nell'ambito dei trattamenti effettuati nella relativa direzione/negli uffici allo stesso sottoposti;

   Questa figura è il riferimento del Titolare, il quale, con il presente Regolamento, impartisce a esso 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 e all'eventuale uso di apparecchiature di videosorveglianza.

   Con il presente Regolamento lo stesso è informato delle responsabilità che gli sono affidate in relazione a quanto disposto dal Codice e dal GDPR.

   Istruzioni:

   Il Designato, in ossequio al GDPR, deve attenersi alle seguenti istruzioni:

   a) verificare la legittimità dei trattamenti di dati personali effettuati dalla direzione di riferimento;
   b) presidiare l'aggiornamento dei registri delle attività di trattamento e il monitoraggio dei rischi per la relativa direzione di competenza, comunicando eventuali eventi potenzialmente dannosi per gli interessati;
   c) predisporre le informative relative al trattamento dei dati personali nel rispetto dell'art. 13-14 del GDPR;
   d) individuare i responsabili esterni e i soggetti autorizzati a compiere operazioni di trattamento (di seguito anche "incaricati") fornendo agli stessi istruzioni per il corretto trattamento dei dati, sovrintendendo e vigilando sull'attuazione delle istruzioni impartite; tale individuazione deve essere effettuata in aderenza alle indicazioni contenute nel presente documento e, in particolare, facendo espresso richiamo alle policy in materia di sicurezza informatica e protezione dei dati personali;
   e) predisporre ogni adempimento organizzativo necessario per gestire le procedure che garantiscano agli interessati l'esercizio dei diritti previsti dalla normativa;
   f) collaborare con il Responsabile per la protezione dei dati al fine di consentire allo stesso l'esecuzione dei compiti e delle funzioni assegnate;
   g) garantire al Responsabile per la protezione dei dati i necessari permessi di accesso ai dati e ai sistemi per l'effettuazione delle verifiche di sicurezza, anche a seguito di incidenti di sicurezza;

   Nell'attuazione dei compiti sopra indicati i soggetti sopra individuati può contattare e acquisire il parere del RPD.

Il Designato, 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 GDPR riguardanti l'adozione di misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio;
- informare il titolare, senza ingiustificato ritardo, della conoscenza dell'avvenuta violazione dei dati personali,

- collaborare nella notificazione di una violazione dei dati personali al Garante privacy, nella comunicazione di una violazione dei dati personali all'interessato, nella redazione della valutazione d'impatto sulla protezione dei dati o nell'eventuale consultazione preventiva.

Il Designato risponde al titolare di ogni violazione o mancata attivazione di quanto dettato dalla normativa vigente e della mancata attuazione delle misure di sicurezza.

Il Designato è destinatario degli interventi di formazione e di aggiornamento.

B. INCARICATI:

Con il presente Regolamento si stabilisce che il personale dipendente del titolare, i tirocinanti, i collaboratori continuativi e/o altri soggetti, che comunque operano sotto l'autorità del Titolare, sono autorizzati, in relazione ai compiti loro conferiti, al trattamento dei dati personali nel rispetto delle mansioni ricoperte e nei limiti delle finalità connesse al rapporto di lavoro con l'Ente, coerentemente con quanto previsto dalle norme vigenti e dalle presenti Linee guida.

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 autorizzato ai sensi dell'art. 2-quaterdecies del Codice nonché ai sensi degli artt. 4 co.10 e art. 29 del GDPR.

Tali soggetti vengo formalmente autorizzati:

1. tramite individuazione nominativa (nome e cognome) delle persone fisiche. In questo caso occorre specificare, per ciascun nominativo, i trattamenti che lo stesso è autorizzato ad effettuare;
2. tramite assegnazione funzionale della persona fisica alla unità organizzativa/Direzione, qualora la persona fisica effettui tutti i trattamenti individuati puntualmente per tale unità.

Nel primo caso, l'autorizzazione scritta deve inoltre contenere le istruzioni impartite agli incaricati del trattamento.

Tali istruzioni, oltre a riguardare eventuali aspetti di dettaglio da diversificare in relazione alle specificità dei singoli trattamenti, devono quanto meno contenere un espresso richiamo alle Linee guida dell'Istituto e alle policy in materia di sicurezza informatica e protezione dei dati personali.

Gli incaricati collaborano con il titolare ed il designato segnalando eventuali situazioni di rischio nel trattamento dei dati e fornendo ogni informazione necessaria per l'espletamento delle funzioni di controllo.

Con il presente Regolamento si impartiscono a 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.

Istruzioni:

In particolare, gli incaricati devono assicurare che, nel corso del trattamento, i dati siano:

- trattati solo nell'ambito delle funzioni ricoperte e dell'attività regolarmente assegnatagli;
- trattati in modo lecito, corretto e trasparente nei confronti dell'interessato;
- trattati con la riservatezza, l'integrità e la disponibilità che la segretezza dell'ufficio richiede;
- 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 e dal designato, nei soli casi previsti dalla legge, nello svolgimento dell'attività istituzionale del titolare.
Gli incaricati dipendenti del titolare possono essere destinatari degli interventi di formazione di aggiornamento.

C. **GLI INCARICATI AL TRATTAMENTO NON DIPENDENTI DEL TITOLARE O PER SPECIFICHE ATTIVITÀ**:
1. Tutti i soggetti che svolgono un'attività di trattamento dei dati, e che non sono dipendenti del titolare (quali a titolo meramente esemplificativo i soggetti che operano temporaneamente all'interno della struttura organizzativa del titolare o che svolgono solo specifici e limitati interventi sui dati personali), devono essere autorizzati nominativamente al trattamento tramite apposito atto scritto di nomina.
2. Questi ultimi sono soggetti agli stessi obblighi a cui sono sottoposti tutti gli incaricati dipendenti del titolare, salvo specifiche istruzioni afferenti al servizio svolto, in modo da garantire il pieno rispetto della tutela della riservatezza dei dati.
3. Gli incaricati non dipendenti dal titolare, valutato caso per caso, possono essere destinatari degli interventi di formazione di aggiornamento.

Art. 18. - Responsabilità in caso di violazione delle disposizioni in materia di protezione dei dati personali

1. Il presente Regolamento, approvato con specifica determina del Titolare, costituisce a tutti gli effetti di legge un regolamento istituzionale che il personale dell'ente deve osservare rigorosamente a pena di comminazione di sanzioni disciplinari così come previste dalla normativa e della Contrattazione Collettiva nazionale relativa al pubblico impiego.
2. Ad ogni modo, ai fini del presente Regolamento si evidenzia che il mancato rispetto delle disposizioni in materia di riservatezza dei dati personali è punito con le sanzioni previste dagli articoli da 166 a 172 del Codice Privacy da parte dell'Autorità di controllo oltre alle sanzioni di natura disciplinare sopra richiamate.
3. Il Titolare del trattamento risponde per il danno cagionato dal suo trattamento con conseguente violazione del presente Regolamento.
4. Il responsabile del trattamento risponde per il danno causato dal trattamento solamente se non abbia adempiuto agli obblighi previsti dal Codice, dal GDPR e dal presente Regolamento e allo stesso specificamente diretti o qualora abbia agito in modo difforme o contrario rispetto alle legittime istruzioni impartitegli dal Titolare.
5. Il Titolare e il responsabile del trattamento sono esonerati da responsabilità se dimostrano che l'evento dannoso non è in alcun modo loro imputabile.

Art. 19. - Responsabile del trattamento (RDT) e sub responsabili

1. Il responsabile è il soggetto che, in ragione di un rapporto giuridico, svolge attività di trattamento dei dati per conto del Titolare.
2. Il responsabile è designato dal Titolare facoltativamente. Ove necessario per esigenze organizzative, possono essere designati responsabili più soggetti, anche mediante suddivisione di compiti. In particolare, il Titolare può avvalersi per il trattamento di dati anche sensibili/particolari, di soggetti pubblici o privati che, in qualità di responsabili del trattamento, forniscano le garanzie del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza. Se nominato, 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.
3. Il Responsabile del trattamento non ricorre a un altro Responsabile senza previa autorizzazione scritta, specifica o generale, del titolare.
4. È consentita la nomina di sub-responsabili del trattamento da parte di ciascun Responsabile del trattamento per specifiche attività di trattamento, nel rispetto degli stessi obblighi contrattuali che legano il Titolare ed il Responsabile primario; le operazioni di trattamento possono essere effettuate solo da incaricati che operano sotto la diretta autorità del Responsabile attenendosi alle istruzioni loro impartite per iscritto che individuano specificatamente l'ambito del trattamento consentito. Il Responsabile risponde, anche dinanzi al Titolare, dell'operato del sub-responsabile anche ai fini del risarcimento di eventuali danni causati dal trattamento, salvo dimostri che l'evento dannoso non gli è in alcun modo imputabile e che ha vigilato in modo adeguato sull'operato del sub-responsabile.
5. Il Responsabile del trattamento garantisce che chiunque agisca sotto la sua autorità ed abbia accesso a dati personali sia in possesso di apposita formazione ed istruzione e si sia impegnato alla riservatezza od abbia un adeguato obbligo legale di riservatezza.
6. Il Responsabile del trattamento dei dati provvede, per il proprio ambito di competenza, a tutte le attività previste dalla legge e a tutti i compiti affidatigli dal Titolare, analiticamente specificati per iscritto nell'atto di designazione, ed in particolare provvede:
   - 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;
   - alla tenuta del registro delle categorie di attività di trattamento svolte per conto del Titolare;
   - ad individuare per iscritto le persone, soggette alla propria autorità e vigilanza, autorizzate al trattamento dei dati personali e dare loro le istruzioni idonee per il trattamento dei dati personali;
   - a conservare gli estremi identificativi delle persone fisiche preposte quali amministratori di sistema, e a fornirli e al titolare su richiesta del medesimo;
   - ad assistere il Titolare nella conduzione della valutazione dell'impatto sulla protezione dei dati (di seguito indicata con "DPIA") fornendo allo stesso ogni informazione di cui è in possesso;
   - ad informare il Titolare, senza ingiustificato ritardo, della conoscenza di casi di violazione dei dati personali (cd. "*data breach*"), per la successiva notifica della violazione al Garante Privacy, nel caso che il Titolare stesso ritenga probabile che dalla violazione dei dati possano derivare rischi per i diritti e le libertà degli interessati;
   - trattare i dati personali, anche di natura sensibile, del Titolare esclusivamente per le finalità previste dal contratto o dalla convenzione;

- 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 di sicurezza adottate per garantire la riservatezza e la protezione dei dati personali trattati.

7. In caso di mancato rispetto delle precedenti disposizioni e di mancata comunicazione al Titolare dell'atto di nomina dei soggetti autorizzati al trattamento, laddove richiesti, risponde direttamente il responsabile del trattamento nei confronti del Titolare. La nomina del responsabile viene effettuata mediante atto da parte del Titolare del trattamento da allegare agli accordi, alle convenzioni o ai contratti che prevedono l'affidamento a soggetti esterni di trattamenti di dati personali.
8. L'accettazione della nomina e l'impegno a rispettare le disposizioni del Codice, del GDPR e del presente Regolamento sono condizioni necessarie per l'instaurazione del rapporto giuridico fra le parti.

Art. 20. - Amministratori di Sistema

1. L' amministratore di sistema sovraintende alla gestione e alla manutenzione delle banche dati e nel suo complesso, al sistema informatico di cui è dotato l'Istituto.
2. La nomina dell'amministratore di sistema deve avvenire previa valutazione dell'esperienza, della capacità e dell'affidabilità del soggetto designato, il quale deve fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento dei dati e in tema di sicurezza. La designazione dell'Amministratore di sistema è individuale e nominativa e deve recare l'elencazione analitica degli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato.
3. L' amministratore di sistema svolge le attività quali il salvataggio dei dati, l'organizzazione dei flussi di rete, la gestione dei supporti di memorizzazione e la manutenzione hardware e propone al Titolare del trattamento un documento di valutazione del rischio informatico.
4. Nel rispetto della normativa in materia di protezione dei dati e della sicurezza, l'amministratore di sistema deve adottare sistemi idonei alla registrazione degli accessi logici ai sistemi di elaborazione e agli archivi elettronici. Le registrazioni (*access log*) devono essere complete, inalterabili, verificabili nella loro integrità e adeguate al raggiungimento dello scopo di verifica per cui sono richieste.
5. Le registrazioni devono comprendere il riferimento temporale e la descrizione dell'evento che le ha generate e devono essere conservate per un periodo congruo non inferiore ai 6 mesi.
6. Secondo la normativa vigente, l'operato dell'amministratore di sistema deve essere verificato con cadenza annuale da parte del Titolare del trattamento, in modo da controllare la rispondenza alle misure tecnico-organizzative e di sicurezza attivate rispetto all'attività di trattamento dei dati personali.
7. Il Titolare di sistema applica le disposizioni impartite dal Garante in materia di misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema.
8. L'amministratore di sistema è destinatario degli interventi di formazione e di aggiornamento.

Art. 21. - Responsabile della protezione dati

1. Il Responsabile della protezione dei dati (RPD) è individuato nella figura unica come persona fisica o giuridica (azienda o *professionista scelti tramite procedura ad evidenza pubblica).*
   L'incaricato persona fisica o giuridica è selezionato mediante procedura ad evidenza pubblica fra soggetti aventi idonee qualità professionali, che abbiano maturato approfondita conoscenza del settore e delle strutture organizzative degli enti locali, nonché delle norme e procedure amministrative agli stessi applicabili; i compiti attribuiti al RPD sono indicati in apposito contratto di servizio.
2. Il RPD è incaricato dei seguenti compiti:

a) informare e fornire consulenza al Titolare e al Designato nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal GDPR e dalle altre normative relative alla protezione dei dati. In tal senso il RPD può indicare al Titolare e/o al Designato i settori funzionali ai quali riservare un *audit* interno o esterno in tema di protezione dei dati, le attività di formazione interna per il personale che tratta dati personali, e a quali trattamenti dedicare maggiori risorse e tempo in relazione al rischio riscontrato;
b) sorvegliare l'osservanza del GDPR e delle altre normative relative alla protezione dei dati, fermo restando le responsabilità del Titolare e del Designato. Fanno parte di questi compiti la raccolta di informazioni per individuare i trattamenti svolti, l'analisi e la verifica dei trattamenti in termini di loro conformità, l'attività di informazione, consulenza e indirizzo nei confronti del Titolare;
c) sorvegliare sulle attribuzioni delle responsabilità, sulle attività di sensibilizzazione, formazione e controllo attuate dal Titolare;
d) fornire, se richiesto, un parere in merito alla valutazione di impatto sulla protezione dei dati (DPIA) e sorvegliarne lo svolgimento. Il Titolare, in particolare, si consulta con il RPD in merito a: se condurre o meno una DPIA; quale metodologia adottare nel condurre una DPIA; se condurre la DPIA con le risorse interne ovvero esternalizzandola; quali salvaguardie applicare, comprese misure tecniche e organizzative, per attenuare i rischi delle persone interessate; se la DPIA sia stata condotta correttamente o meno e se le conclusioni raggiunte (procedere o meno con il trattamento, e quali salvaguardie applicare) siano conformi al GDPR;
e) cooperare con il Garante per la protezione dei dati personali e fungere da punto di contatto per detta Autorità per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'art. 36 GDPR, ed effettuare, se del caso, consultazioni relativamente a ogni altra questione. A tali fini il nominativo del RPD è comunicato dal Titolare e/o dal Designato al Garante;
f) verificare la tenuta e l'aggiornamento dei registri di cui ai successivi artt. 9 e 10.

3. Il Titolare ed il Designato assicurano che il RPD sia tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali. A tal fine:
   - il RPD deve disporre tempestivamente di tutte le informazioni pertinenti sulle decisioni che impattano sulla protezione dei dati, in modo da poter rendere una consulenza idonea, scritta od orale;
   - il parere del RPD sulle decisioni che impattano sulla protezione dei dati è obbligatorio ma non vincolante. Nel caso in cui la decisione assunta determina condotte difformi da quelle raccomandate dal RPD, è necessario motivare specificamente tale decisione;
   - il RPD deve essere consultato tempestivamente qualora si verifichi una violazione dei dati o un altro incidente.
4. Nello svolgimento dei compiti affidatigli il RPD deve debitamente considerare i rischi inerenti al trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo.
5. La figura di RPD è incompatibile con chi determina le finalità od i mezzi del trattamento; in particolare, risultano con la stessa incompatibili:
   - il Responsabile per la prevenzione della corruzione e per la trasparenza;
   - il Responsabile del trattamento;
   - qualunque incarico o funzione che comporta la determinazione di finalità o mezzi del trattamento.
6. Il Titolare e il Designato forniscono al RPD le risorse necessarie per assolvere i compiti attribuiti e garantiscono l'accesso ai dati personali ed ai trattamenti. In particolare, è assicurato al RPD:
   - supporto attivo per lo svolgimento dei compiti da parte del Titolare e/o del Designato, anche considerando l'attuazione delle attività necessarie per la protezione dati;

- tempo sufficiente per l'espletamento dei compiti affidati al RPD;
- supporto adeguato in termini di infrastrutture (sede, attrezzature, strumentazione);
- comunicazione ufficiale della nomina a tutto il personale, in modo da garantire che la sua presenza e le sue funzioni siano note all'interno dell'Ente;
- accesso garantito ai settori funzionali dell'Ente così da fornirgli supporto, informazioni e input essenziali.

7. Il RPD opera in posizione di autonomia nello svolgimento dei compiti allo stesso attribuiti; in particolare, non deve ricevere istruzioni in merito al loro svolgimento né sull'interpretazione da dare a una specifica questione attinente alla normativa in materia di protezione dei dati.
8. Ferma restando l'indipendenza nello svolgimento di detti compiti, il RPD riferisce direttamente al Titolare od al Designato.
9. Nel caso in cui siano rilevate dal RPD o sottoposte alla sua attenzione decisioni incompatibili con il GDPR e con le indicazioni fornite dallo stesso RPD, quest'ultimo è tenuto a manifestare il proprio dissenso, comunicandolo al Titolare ed al Designato.
10. Il RPD non può essere rimosso o penalizzato dal Titolare e dal Designato per l'adempimento dei propri compiti.

CAPO IV SICUREZZA DEI DATI PERSONALI

Art. 22. - Misure di sicurezza

1. L'adozione di adeguate misure di sicurezza è lo strumento fondamentale per garantire la tutela dei diritti e delle libertà delle persone fisiche. Il livello di sicurezza è valutato tenuto conto dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati. L'efficace protezione dei dati personali è perseguita sia al momento di determinare i mezzi del trattamento (fase progettuale) sia all'atto del trattamento.
2. Il Polo scolastico 2 – Liceo scientifico "Torelli" – Fano e Pergola (PU) mette in atto misure tecniche ed organizzative idonee a garantire un livello di sicurezza adeguato al rischio tenendo conto dei costi di attuazione, nonché della natura, del campo di applicazione, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche.
3. Le misure tecniche ed organizzative di sicurezza da mettere in atto per ridurre i rischi del trattamento ricomprendono: la pseudonimizzazione, la minimizzazione, la cifratura dei dati personali, la capacità di assicurare la continua riservatezza, integrità, disponibilità e resilienza dei sistemi e dei servizi che trattano i dati personali, la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati in caso di incidente fisico o tecnico, una procedura per provare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.
4. Costituiscono misure tecniche ed organizzative che possono essere adottate dal Servizio cui è preposto il Designato:
   - sistemi di autenticazione; sistemi di autorizzazione; sistemi di protezione (antivirus; firewall; antintrusione; altro);
   - misure antincendio; sistemi di rilevazione di intrusione; sistemi di sorveglianza; sistemi di protezione con videosorveglianza; registrazione accessi; porte, armadi e contenitori dotati di serrature e ignifughi; sistemi di copiatura e conservazione di archivi elettronici;
   - altre misure per ripristinare tempestivamente la disponibilità e l'accesso dei dati in caso di incidente fisico o tecnico.

5. La conformità del trattamento dei dati al GDPR in materia di protezione dei dati personali è dimostrata attraverso l'adozione delle misure di sicurezza o l'adesione a codici di condotta approvati o ad un meccanismo di certificazione approvato.
6. Il Polo scolastico 2 – Liceo scientifico "Torelli" – Fano e Pergola (PU) e/o il Designato si obbligano ad impartire adeguate istruzioni sul rispetto delle predette misure a chiunque agisca per loro conto ed abbia accesso a dati personali.
7. I nominativi ed i dati di contatto del Titolare, e del Responsabile della protezione dati sono pubblicati sul sito istituzionale del Titolare, sezione Amministrazione trasparente, oltre che nella sezione "Privacy" costituita.
8. Restano in vigore le misure di sicurezza attualmente previste per i trattamenti di dati sensibili per finalità di rilevante interesse pubblico nel rispetto degli specifici regolamenti attuativi (ex artt. 20 e 22, D.lgs. n. 196/2003).

Art. 23. - Registro delle attività di trattamento

1. Il Titolare del trattamento istituisce un registro, anche in formato digitale, delle attività di trattamento e delle categorie di trattamenti svolte sotto la propria responsabilità nel rispetto dell'art. 30 GDPR.
2. Il Registro delle attività di trattamento svolte dal Titolare o dal Designato reca almeno le seguenti informazioni:
   a) il nome ed i dati di contatto dell'Istituto, del Dirigente Scolastico, eventualmente del Contitolare del trattamento, del RPD;
   b) le finalità del trattamento;
   c) la sintetica descrizione delle categorie di interessati, nonché le categorie di dati personali;
   d) le categorie di destinatari a cui i dati personali sono stati o saranno comunicati;
   e) l'eventuale trasferimento di dati personali verso un paese terzo od una organizzazione internazionale;
   f) ove stabiliti, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
   g) il richiamo alle misure di sicurezza tecniche ed organizzative del trattamento adottate, come da precedente art. 22.
3. Il Titolare, per il tramite di ciascun soggetto dallo stesso designato, conserva presso gli uffici della struttura organizzativa del Titolare, in forma telematica/cartacea, il Registro.
4. Il Designato ha la responsabilità della regolare tenuta e aggiornamento del Registro delle attività di trattamento con riferimento agli ambiti di competenza.
5. Qualora l'organizzazione svolga l'attività di trattamento in qualità di responsabile esterno, adotta il registro delle attività di trattamento svolte per conto di un Titolare.

Art. 24. - Valutazioni d'impatto sulla protezione dei dati

1. 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.
2. La DPIA è uno strumento importante per la responsabilizzazione del Titolare in quanto consente allo stesso non soltanto di rispettare i requisiti previsti dal GDPR ma anche di dimostrare che sono state adottate misure appropriate per garantire il rispetto dello stesso.
3. La DPIA sulla protezione dei dati personali deve essere realizzata prima di procedere al trattamento dal Titolare quando un tipo di trattamento, consideratane la natura, il contesto e le finalità, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche. Per "rischio" si intende 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 al fine di indirizzare e controllare un'organizzazione.

4. Prioritariamente alla DPIA deve:
   - essere effettuata o aggiornata la ricognizione dei trattamenti;
   - essere effettuata la determinazione in ordine alla possibilità che il trattamento possa causare un rischio elevato per i diritti e le libertà degli interessati.
5. La DPIA deve essere effettuata - con eventuale riesame delle valutazioni condotte - anche per i trattamenti in corso che possano presentare un rischio elevato per i diritti e le libertà delle persone fisiche, nel caso in cui siano intervenute variazioni dei rischi originari tenuto conto della natura, dell'ambito, del contesto e delle finalità del medesimo trattamento.
6. Il Titolare del trattamento, nello svolgere l'attività di valutazione, si consulta con il responsabile della protezione dei dati personali. 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 GDPR.

Art. 25. - Violazione dei dati personali

1. Per violazione dei dati personali (in seguito "data breach") si intende la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso non autorizzato ai dati personali trasmessi, conservati o comunque trattati dal Titolare.
2. Ogni dipendente che venga a conoscenza di una violazione dei dati personali è tenuto a segnalarlo al titolare e/o al designato che deve comunicarlo al RPD al fine di provvedere ai sensi del presente articolo.
3. Il Titolare, ove ritenga probabile che dalla violazione dei dati possano derivare rischi per i diritti e le libertà degli interessati, provvede alla notifica della violazione al Garante Privacy 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 non sia effettuata entro 72 ore, è corredata dei motivi del ritardo.
4. I principali rischi per i diritti e le libertà degli interessati conseguenti ad una violazione, in conformità al considerando 75 del GDPR, sono i seguenti:
   - danni fisici, materiali o immateriali alle persone fisiche;
   - perdita del controllo dei dati personali;
   - limitazione dei diritti, discriminazione;
   - furto o usurpazione d'identità;
   - perdite finanziarie, danno economico o sociale;
   - decifratura non autorizzata della pseudonimizzazione;
   - pregiudizio alla reputazione;
   - perdita di riservatezza dei dati personali protetti da segreto professionale (sanitari, giudiziari).
5. Se il Titolare ritiene che il rischio per i diritti e le libertà degli interessati conseguente alla violazione rilevata è elevato, allora deve informare questi ultimi, "senza ingiustificato ritardo", con un linguaggio semplice e chiaro al fine di fare comprendere loro la natura della violazione dei dati personali verificatesi. Non è richiesta la comunicazione agli interessati laddove siano soddisfatte almeno una delle condizioni indicate al paragrafo 3 dell'art. 34.
6. I rischi per i diritti e le libertà degli interessati possono essere considerati "elevati" quando la violazione può, a titolo di esempio:
   - coinvolgere un rilevante quantitativo di dati personali e/o di soggetti interessati;
   - riguardare categorie particolari di dati personali;

- comprendere dati che possono accrescere ulteriormente i potenziali rischi (ad esempio dati di localizzazione, finanziari, relativi alle abitudini e preferenze);
- comportare rischi imminenti e con un'elevata probabilità di accadimento (ad esempio rischio di perdita finanziaria in caso di furto di dati relativi a carte di credito);
- impattare su soggetti che possono essere considerati vulnerabili per le loro condizioni (ad esempio, utenti deboli, minori, soggetti indagati).

7. La notifica deve avere il contenuto minimo previsto dall'art. 33 GDPR, ed anche la comunicazione all'interessato deve contenere almeno le informazioni e le misure di cui al citato art. 33.
8. Il Titolare dovrà in ogni caso documentare le violazioni di dati personali subite, anche se non notificate all'Autorità Garante e non comunicate agli interessati, nonché le relative circostanze e conseguenze e i provvedimenti adottati così come indicato dall'art. 33, paragrafo 5 GDPR.
9. La documentazione di cui al punto precedente dovrà essere messa a disposizione dell'Autorità qualora richiesto.
10. Il Titolare deve opportunamente documentare le violazioni di dati personali subite, anche se non comunicate alle autorità di controllo, nonché le circostanze ad esse relative, le conseguenze e i provvedimenti adottati o che intende adottare per porvi rimedio. Tale documentazione deve essere conservata con la massima cura e diligenza in quanto può essere richiesta dal Garante Privacy al fine di verificare il rispetto delle disposizioni del GDPR.
11. Il responsabile del trattamento informa il Titolare del trattamento senza ingiustificato ritardo dopo essere venuto a conoscenza della violazione.

Art. 26. - Procedura in caso di accertamento ispettivo o richieste istruttorie da parte dell'Autorità

1. Si premette che, a seguito di adesione a specifico protocollo di intesa del 10 marzo 2016, l'Autorità Garante può avvalersi della Guardia di finanza, per il tramite del Nucleo Speciale Tutela Privacy e Frodi Tecnologiche, per attuare attività ispettiva delegata o congiunta in tema di dati personali. I poteri di indagine sono disciplinati dall'art. 58 GDPR, in cui al secondo paragrafo sono indicati anche i poteri correttivi.
2. L'attività ispettiva è ulteriormente specificata dagli artt. 157 e ss. del Codice Privacy.
3. L'attività ispettiva e ogni ulteriore richiesta da parte dell'Autorità garante richiede una cooperazione totale tra Titolare, RPD e Autorità stessa.
4. In ragione di ciò, laddove dovesse pervenire una richiesta da parte dell'Autorità o ci fosse un'attività ispettiva è necessario che il Titolare sia pronto a rispondere a ogni richiesta, nel rispetto del principio dell'accountability, che fonda l'intera struttura del GDPR.
5. La presenza del Responsabile per la protezione dei dati (RPD) è necessaria e fondamentale, anche per fare da intermediario tra il Titolare e l'Autorità. Pertanto, dovrà essere convocato subito e, se assolutamente impossibilitato per ragioni oggettive, laddove non si possa posticipare l'incombente, lo stesso potrà individuare un suo idoneo sostituto.
6. In prima battuta, all'Autorità dovrà essere presentate e illustrato il presente Regolamento adottato dal Titolare in materia di dati personali. Dopodiché il Titolare dovrà avere a disposizione i documenti che attestino l'attività svolta in materia di protezione dei dati.
   Si raccomanda la piena collaborazione.

Art. 27. - Regole di comportamento con riguardo alla protezione dei dati personali

1. Trattare un dato personale vuol dire compiere qualunque operazione o complesso di operazioni con o senza l'ausilio di strumenti elettronici. Il trattamento di un dato personale, per essere lecito, corretto e trasparente, deve sempre avvenire secondo i principi generali a tutela della privacy, che possono essere considerati vincoli inscindibili al trattamento dei dati personali.
2. Si stabiliscono, pertanto, le regole relative alla:
   a. gestione dei locali e delle risorse fisiche

   a.1. Tutti i locali e tutte le risorse fisiche del **Titolare** devono essere utilizzati e custoditi con la massima diligenza al fine di garantire un'efficiente conduzione dell'attività lavorativa ed un elevato livello di sicurezza delle informazioni.

   a.2. L'accesso agli uffici, alle aree riservate ed agli archivi cartacei è permesso agli utenti autorizzati muniti di badge personale, in base a precise e motivate esigenze lavorative.

   a.3. I visitatori e gli ospiti di vario tipo potranno avere accesso agli uffici comunali esclusivamente dietro autorizzazione dell'addetto alla portineria.

   a.4. L'accesso ai locali del Data Center è permesso esclusivamente a personale autorizzato munito della relativa chiave ed, in via eccezionale, agli addetti al controllo e alla manutenzione dello stesso opportunamente accompagnati dal personale interno competente.

   b. gestione della postazione di lavoro e dei dati in generale

   b.1. L'utilizzo della postazione di lavoro e il conseguente accesso ai documenti, atti e archivi è consentito nei limiti della propria funzione e dei propri incarichi.

   b.2. La propria scrivania deve essere mantenuta in ordine, verificando di non lasciare documenti e atti riservati disponibili all'accesso di terzi n momenti di pausa, terminata la giornata di lavoro e/o in periodi di assenza.

   b.3. I documenti cartacei necessari per lo svolgimento delle mansioni lavorative devono essere custoditi in armadi o cassettiere. I documenti devono essere riposti correttamente durante i periodi di temporanea assenza ed al termine dell'attività lavorativa negli appositi archivi.

   b.4. I documenti e gli atti contenenti dati particolari devono essere custoditi in armadi chiusi a chiave.

   b.5. L'eliminazione fisica di ogni documento cartaceo o supporto informatico contenente dati e informazioni istituzionali e/o personali deve essere effettuata solo utilizzando gli appositi strumenti e nel rispetto di quanto previsto nel Manuale di Gestione documentale dell'Ente.

   b.6. Si raccomanda di non lasciare documenti incustoditi presso i dispositivi di stampa e di distruggere personalmente le stampe quando non servono più.

   b.7. Ogni utente è responsabile dei dati e delle informazioni delle quali entra in possesso per lo svolgimento della sua attività lavorativa. Deve quindi adottare ogni idonea misura di sicurezza al fine di tutelarne la riservatezza, la sicurezza, l'integrità e il corretto utilizzo.

   b.8. I dati e le informazioni possono essere comunicati a terze parti esclusivamente nell'ambito della propria funzione e secondo le modalità connesse alla propria attività lavorativa.

   b.9. È vietata la comunicazione di dati e di informazioni verso terzi che possano arrecare danno all'immagine, alla reputazione, alla produttività, alla proprietà intellettuale e alla efficacia ed efficienza dell'attività dell'Ente o che possano violare i vincoli contrattuali e di legge connessi al rapporto di lavoro.

   b.10. È assolutamente vietata la divulgazione a terzi di informazioni riservate, confidenziali o comunque di proprietà del Titolare. In caso di violazione, il Titolare si riserva di avviare i relativi provvedimenti disciplinari, nonché le azioni civili e penali consentite.

b.11. La diffusione illecita di dati e informazioni potrebbe configurare, oltre alla violazione del presente Regolamento, la violazione di norme con conseguenze sia civili che penali a carico del responsabile dell'illecita diffusione, nonché come violazione della normativa che regola il rapporto di lavoro.

b.12. In caso di furto o smarrimento di fascicoli o atti contenenti dati personali l'utente deve informare immediatamente per iscritto il Titolare e/o il Designato. Dovrà altresì informare il Responsabile Protezione Dati.

c. degli strumenti informatici

c.1. Per la gestione degli strumenti informatici si fa riferimento a quanto stabilito dal Regolamento per l'utilizzo degli strumenti informatici e dalle singole procedure IT ad esso allegate.

Art. 28. - Rinvio

1. Per quanto non previsto nel presente Regolamento si applicano le disposizioni del Codice, del GDPR, le Linee guida e i provvedimenti del Garante.
2. Il presente Regolamento è aggiornato a seguito di ulteriori modificazioni alla vigente normativa in materia di riservatezza e protezione dei dati personali.