**Ministero dell'Istruzione**
**ISTITUTO COMPRENSIVO STATALE DI SCUOLA DELL'INFANZIA, PRIMARIA E SECONDARIA DI PRIMO GRADO**
via Lina Schwarz, 6 21051 ARCISATE (VA)
Tel 0332 470122 – fax 0332 471854
codice ministeriale: vaic81800e – codice fiscale: 80018000127
sito internet: www.ics-arcisate.edu.it
email: vaic81800e@istruzione.it
email posta certificata: vaic81800e@pec.istruzione.it

Al personale docente e ATA
dell'Istituto Comprensivo
Loro sedi

Oggetto: Trasmissione Documentazione Privacy

Si trasmette in allegato il manuale sulla privacy e il documento sulla privacy policy.
Sarà inviata successivamente la nomina di incarico al trattamento dei dati personali ai sensi del Regolamento UE 2016/679 (GDPR).

Cordiali saluti

IL DIRIGENTE SCOLASTICO
PROF. WALTER FIORENTINO
(Documento firmato digitalmente ai sensi del c.d.
Codice dell'Amministrazione Digitale e norme ad esso connesse)

**Ministero dell'Istruzione, dell'Università e della Ricerca**
**ISTITUTO COMPRENSIVO STATALE DI SCUOLA DELL'INFANZIA, PRIMARIA E SECONDARIA DI PRIMO GRADO**
Via Lina Schwarz, 6 – 21051 ARCISATE (VA)
Tel: 0332 470122 - Fax: 0332 471854
codice ministeriale: vaic81800e – codice fiscale: 80018000127
sito internet: www.ics-arcisate.edu.it
email: vaic81800e@istruzione.it
email posta certificata: vaic81800e@pec.istruzione.it

# Privacy Policy

## Sommario

## 1. Scopo e definizioni del documento

Lo scopo del presente documento è definire il modello Privacy, ovvero individuare le disposizioni operative interne volte a disciplinare il trattamento dei dati personali effettuato dalla Scuola, ai sensi del Regolamento UE n. 679 del 2016 e del D. Lgs. n. 169/03 come modificato dal D. Lgs. 10 agosto 2018 n. 101, nonché ulteriori provvedimenti in materia di fonte normativa secondaria, in vigore al momento dell'approvazione della seguente policy. In essa sono quindi disciplinati i ruoli e le responsabilità nonché gli adempimenti da seguire in materia di protezione dei Dati Personali ai sensi del "Codice Privacy" e del "GDPR", anche con riferimento alle decisioni e ai provvedimenti emessi dall'Autorità Garante per la protezione dei dati personali.

Ai fini della presente Policy si applicano le seguenti definizioni, coerenti con quanto previsto dalla normativa di settore:

- **Regolamento**: Regolamento (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, che abroga la direttiva 95/46/CE (c.d GDPR - Regolamento Generale sulla Protezione dei Dati);
- **Normativa**: D. Lgs. n. 169 del 2003 come modificato dal D. Lgs. 10 agosto 2018 n. 101 e Regolamento UE n. 679 del 2016, nonché ulteriori provvedimenti in materia di fonte normativa secondaria in vigore al momento dell'approvazione della seguente policy.
- **Codice Privacy**: Decreto legislativo 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali";
- **Scuola**: ISTITUTO COMPRENSIVO STATALE DI SCUOLA DELL'INFANZIA, PRIMARIA E SECONDARIA DI PRIMO GRADO - Via Lina Schwartz, 6 – 21051 ARCISATE (VA);
- **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;
- **Dato personale**: 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;
- **Dati di categorie particolari**: dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché 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.
- **Dati genetici**: i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione;
- **Dati biometrici**: i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici;

- **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;
- **Interessato**: la persona fisica cui si riferiscono i dati personali;  Responsabile del trattamento: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;
- **Autorizzato**: la persona fisica autorizzata a compiere operazioni di trattamento dal Titolare o dal Responsabile (detta anche "incaricato al trattamento" o "addetto al 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;
- **Paesi terzi**: paesi non appartenenti all'UE o allo spazio Economico Europeo (Norvegia, Islanda, Liechtenstein);
- **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;

## 2. Principi, ambito di applicazione e destinatari della policy

Il presente documento si applica a tutti i trattamenti di dati personali svolti, manualmente o mediante strumenti automatizzati, da questa Istituzione scolastica in qualità di Titolare del trattamento.

Questa Istituzione scolastica si impegna a garantire e dimostrare che il trattamento dei dati avviene in maniera conforme a quanto previsto dalla normativa e secondo i seguenti principi di liceità di trattamento:

- trattati in modo lecito, corretto e trasparente nei confronti dell'interessato;
- raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità;
- adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati;
- esatti e, se necessario, aggiornati; a tal proposito sono state adottate 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 al conseguimento delle finalità per le quali sono trattati;
- 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.

La stessa garanzia di protezione e di adozione di adeguate misure di sicurezza è richiesta altresì a quei soggetti terzi ai quali la Scuola ha affidato l'incarico della gestione di alcuni trattamenti. A tal fine la policy in oggetto è resa disponibile ai soggetti nominati "Responsabili del trattamento".

Tale policy si applica anche a tutti i Soci, ai dipendenti di questa Istituzione scolastica ed a tutti i soggetti che collaborano a vario titolo col Titolare del trattamento.

## 3. Oggetto e modalità di applicazione

Oggetto della presente Policy è il trattamento dei Dati Personali, anche eventualmente detenuti all'estero, effettuato da questa Istituzione scolastica. Sono esclusi dall'ambito di applicazione i trattamenti dei Dati Personali effettuati da persone fisiche per fini esclusivamente personali e nei casi in cui i dati non sono destinati ad una comunicazione sistematica o alla diffusione (anche se utilizzati ai fini di esigenze di lavoro: ad esempio, banca dati su PC accessibile ed utilizzata solo ed esclusivamente dall'utente - persona fisica per un'elaborazione personale - rubrica telefonica).

## 4. Organigramma e sistema di nomine e responsabilità

Al fine di garantire la tutela dei diritti delle persone fisiche relativamente al trattamento dei dati personali, la Scuola ha implementato un sistema di nomine e ripartizione delle responsabilità di seguito delineate, parametrate alla natura, all'ambito di applicazione, al contesto e alle finalità del trattamento, nonché ai rischi per i diritti e le libertà delle persone fisiche analizzati, come riportato nell'organigramma privacy allegato sotto la lettera "A" alla presente Policy Privacy.

### 4.2 Organigramma privacy dell'Istituto

| | |
|---|---|
| Organigramma valido al | maggio 2019 |
| Titolare del trattamento | ISTITUTO COMPRENSIVO STATALE DI SCUOLA DELL'INFANZIA, PRIMARIA E SECONDARIA DI PRIMO GRADO<br>Via Lina Schwartz, 6 – 21051 ARCISATE (VA)<br>legale rappresentante: Fiorentino Walter - DS |
| Responsabili del trattamento | Elenco dei soggetti esterni |
| Addetti al trattamento | DS<br>DSGA<br>Personale ATA<br>Personale docente<br>Organi collegiali |

### 4.2 Titolare del Trattamento

Conformemente a quanto previsto dalla normativa, Titolare del trattamento è l'ISTITUTO COMPRENSIVO STATALE DI SCUOLA DELL'INFANZIA, PRIMARIA E SECONDARIA DI PRIMO GRADO, Via Lina Schwartz, 6 – 21051 ARCISATE (VA) che si impegna a:

- adeguare il proprio assetto organizzativo per il governo della privacy;
- adottare le modalità operative connesse con la gestione degli adempimenti ed il trattamento dei dati ai fini privacy;
- assumere le decisioni in ordine alle finalità, alle modalità del trattamento dei dati e agli strumenti utilizzati, ivi compreso il profilo della sicurezza, sia per i trattamenti svolti all'interno che all'esterno della propria struttura;
- individuare e designare i Responsabili del trattamento dei dati, impartendo loro le relative istruzioni;
- vigilare sulla puntuale osservanza delle disposizioni e istruzioni impartite, anche nei confronti dei Responsabili del trattamento (sia interni che esterni).

Questa istituzione scolastica, inoltre, si impegna a garantire l'esercizio dei diritti degli interessati e a tal scopo, ha implementato apposite procedure al fine di informare gli interessati dell'esistenza dei seguenti diritti:

- diritto di ottenere la conferma dell'esistenza o meno di dati personali che la riguardano e di averne accesso; c.d. diritto all'accesso. In particolare l'interessato ha diritto di conoscere l'origine dei dati personali; le finalità e modalità del trattamento; la logica applicata in caso di trattamento effettuato con l'ausilio di strumenti elettronici; gli estremi identificativi del titolare, dei responsabili e del rappresentante designato; l'elenco dei soggetti o delle categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di rappresentante designato nel territorio dello Stato, di responsabili o incaricati;
- diritto di ottenere l'aggiornamento, la rettificazione ovvero, quando vi ha interesse, l'integrazione dei dati; c.d. diritto alla rettifica;
- diritto di ottenere la cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge, compresi quelli di cui non è necessaria la conservazione in relazione agli scopi per i quali i dati sono stati raccolti o successivamente trattati; c.d. diritto alla cancellazione;

- diritto di limitare od opporsi, per motivi legittimi, al trattamento, rivolgendosi al personale espressamente incaricato; c.d. diritto di opposizione.

Al fine di esercitare i diritti sopra descritti, questa Istituzione scolastica si impegna a rispondere senza ritardo alle richieste presentate da parte dell'interessato ai Responsabili o agli Incaricati nominati, in forma orale o attraverso ulteriori idonei strumenti.

### 4.3 Responsabile del Trattamento

Il responsabile del trattamento dei dati è la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento.

Il Titolare del trattamento può ricorrere facoltativamente ad uno o più responsabili del trattamento;

Tale soggetto viene individuato in quanto dotato di adeguate garanzie e tra le sue funzioni sono comprese:

- osservare le procedure in materia di protezione dei dati personali adottate dal Titolare;
- organizzare, gestire e supervisionare tutte le operazioni di trattamento dei dati personali affinché esse vengano effettuate nel rispetto delle disposizioni di legge e predisporre tutti i documenti nonché le misure tecniche e organizzative richiesti dal Codice e dal Regolamento;
- adottare e verificare il rispetto delle misure di sicurezza e la conformità dei sistemi e delle misure di sicurezza;
- redigere e aggiornare il registro delle attività di trattamento;
- informare il Titolare del trattamento di tutte le misure adottate e contribuire alle attività di revisione, comprese le ispezioni, realizzate dal Titolare del trattamento o da un altro soggetto da questi incaricato;
- nominare gli incaricati che svolgono le funzioni di amministratore di sistema, conservando i relativi estremi identificativi, definendo gli ambiti di operatività ai medesimi consentiti e verificando almeno annualmente il relativo operato per controllarne la rispondenza alle misure organizzative, tecniche e di sicurezza riguardanti il trattamento dei dati personali;
- inviare, con periodicità stabilita dal Titolare, una lista aggiornata dei nominativi e degli ambiti di operatività degli amministratori di sistema, in particolare al fine di consentire al Titolare l'adempimento dell'obbligazione posta a suo carico dal Provvedimento del Garante Privacy del 27.11.2008 (art. 4.3);
- conferire alle persone autorizzate al trattamento apposite istruzioni sulle norme e le procedure da osservare e provvedere alla relativa formazione, ai sensi dell'art. 29 del Regolamento UE 2016/679;
- controllare le operazioni di trattamento svolte dagli incaricati e la conformità all'ambito di trattamento consentito;
- redigere e aggiornare la lista dei nominativi degli autorizzati e verificarne almeno annualmente l'ambito del trattamento consentito ai medesimi;
- mantenere aggiornato il Titolare del trattamento circa il ricorso ad ulteriori Responsabili del trattamento (sub-responsabili) in relazione all'affidamento agli stessi di determinate attività, in modo da consentire al Titolare del trattamento il mantenimento del controllo sui dati affidati;
- attuare gli obblighi di informazione ed acquisizione del consenso, quando richiesto, nei confronti degli interessati;
- assista per quanto possibile il Titolare del trattamento nell'obbligo di garantire all'interessato che ne faccia richiesta l'effettivo esercizio dei diritti previsti dalla normativa vigente;

- distruggere i dati personali alla fine dei trattamenti degli stessi nei casi previsti dal Regolamento, secondo le procedure atte a garantire la sicurezza degli stessi e provvedere alle formalità di legge e agli adempimenti necessari anche mediante comunicazione al Garante, se dovuta;
- comunicare immediatamente al titolare non oltre le 24 ore successive al loro ricevimento, ogni richiesta, ordine o attività di controllo da parte del Garante o dell'Autorità Giudiziaria;
- osservare le procedure in materia di protezione dei dati personali adottate dal Titolare;
- informare l'interessato del trasferimento dei dati all'estero.

### 4.4 Autorizzati al Trattamento

Il Titolare ha provveduto a nominare, presso le Unità Organizzative in cui vengono svolti i trattamenti, le persone autorizzate al trattamento dei dati.

L'Autorizzato effettua tutte le operazioni di Trattamento dei Dati Personali attinenti all'attività lavorativa di competenza dell'area di appartenenza ed opera sotto l'autorità del Titolare del Trattamento, attenendosi alle istruzioni dallo stesso impartite nonché alle specifiche procedure che regolamentano le modalità di utilizzo delle banche dati cui lo stesso abbia accesso.

In particolare, i compiti ad esso attribuiti sono così sintetizzati:

- segnalare eventuali richieste ricevute da parte dell'interessato sull'esercizio dei relativi diritti, nonché attenersi alla procedura interna sull'esercizio dei diritti;
- avvisare nel caso in cui nello svolgimento di un'attività dovesse riscontrare il trattamento di nuovi dati e finalità per cui risultasse necessario aggiornare il registro dei trattamenti, in applicazione del principio di privacy by design e by default;
- informare immediatamente qualora le istruzioni le risultino non conformi alla normativa sulla protezione dai dati;
- segnalare eventuali accessi non autorizzati;
- rilasciare all'interessato l'informativa e acquisire il consenso laddove necessario, secondo le istruzioni impartite dal Titolare.

## 5. Impegno alla riservatezza

Questa Istituzione scolastica, in qualità di Titolare del trattamento dei dati, garantisce la riservatezza dei dati personali acquisiti e trattati nel corso della propria attività, impegnando contrattualmente alla riservatezza tutti i soggetti che accedono a tali dati per suo conto o sotto la propria autorità.

Le comunicazioni dei dati personali all'interno dell'organizzazione sono regolamentate dal titolare del trattamento in modo che a dati siano disponibili solo per i soggetti autorizzati ad accedervi o perché preventivamente autorizzati, o in forza di una nomina a Responsabile del trattamento, o perché la comunicazione sia necessaria per obblighi di legge, come nel caso di:

- autorità di Vigilanza, italiane o estere, nei casi e con le limitazioni previste dalla legge;
- autorità Amministrativa, giudiziaria e fiscale, nei casi e con le limitazioni previsti dalla legge;
- providers di servizi e/o consulenti tecnico-informatici, anche in Paesi terzi non comunitari, unicamente per esigenze tecniche connesse all'utilizzo da parte del Titolare di sistemi e/o applicazioni strumentali nell'esecuzione degli obblighi contrattuali assunti nell'ambito dell'incarico in oggetto e dei correlati obblighi di legge, fermo restando che il ricorso a tali soggetti avverrà

previo impegno da parte loro a rispettare tutte le prescrizioni in materia di sicurezza dei dati previste dal Codice e dal Regolamento.

Qualora si trovi ad operare in qualità di Responsabile del trattamento per conto di un altro Titolare, questa Istituzione scolastica si impegna a garantire gli standard indicati nelle disposizioni in oggetto nei confronti dei terzi con la medesima diligenza e livello di protezione utilizzati per la sicurezza e la riservatezza dei propri dati.

## 6. Trattamento dei dati personali (definizione e mappatura dei trattamenti)

Secondo quanto previsto dal Regolamento UE 2016/679 (art.30), il Titolare ed eventualmente, il Responsabile se nominato, sono tenuti alla redazione e all'aggiornamento del registro dei trattamenti, da sottoporre all'Autorità di controllo, laddove richiesto.

Il predetto registro deve contenere:

a) il nome e i dati di contatto del Titolare del trattamento e, ove applicabile, del contitolare del trattamento, del Rappresentante esterno del trattamento, del DPO di Gruppo e del Referente esecutivo per la protezione dei dati personali;

b) le finalità del trattamento;

c) una descrizione delle categorie di interessati e delle categorie di dati personali;

d) le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi od organizzazioni internazionali;

e) 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, la documentazione delle garanzie adeguate;

f) ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;

g) ove possibile, una descrizione generale delle misure di sicurezza tecniche.

Il Registro delle attività di trattamento di questa Istituzione scolastica è stato redatto ed è disponibile come documento autonomo nel Sistema di Gestione Privacy dell'Istituto.

## 7. Misure di sicurezza e relativi controlli

### 7.1 La gestione della sicurezza: ruoli e responsabilità

La responsabilità dell'attività di impostazione e coordinamento dei sistemi che garantiscono la sicurezza e la tutela di tutti i dati oggetto di trattamento dell'Istituto sia da un punto di vista logico che fisico, la loro gestione diretta o tramite fornitori, sono in carico al Responsabile IT.

L'amministratore della sicurezza logica segue i seguenti criteri generali:

- in base alle figure professionali presenti in questo Istituto, vengono definiti i profili standard da assegnare agli utenti con le autorizzazioni necessarie all'espletamento delle rispettive mansioni definite per ruoli e competenze;

- la validità delle richieste di accesso alla rete è verificata automaticamente dal sistema stesso prima di consentire l'accesso ai dati, tramite un sistema di autenticazione costituito da User-ID e password.

### 7.2 Misure di controllo dell'accesso ai dati

Sono le misure di sicurezza volte a minimizzare i rischi che le informazioni siano rivelate o modificate senza autorizzazione, ovvero perse o alterate accidentalmente o intenzionalmente. Il sistema in atto prevede un sistema di autenticazione, basato su codice identificativo e password individuale segreta, per assicurare che la persona che accede al sistema, nelle sue diverse articolazioni, sia identificata con certezza, nonché un sistema di autorizzazione, che prevede che a ciascuna persona che accede al sistema sia assegnato un profilo di accesso che definisce i dati ai quali l'utente è autorizzato ad accedere e, ove applicabile, le operazioni che per ciascun dato o gruppo di dati è autorizzato ad eseguire (consultazione, inserimento, modifica, cancellazione). Nessun dipendente di questa Istituzione scolastica è amministratore di sistema della propria macchina.

### 7.3 Clean Desk Policy

La politica di "scrivania pulita" è una delle migliori strategie da attuare quando si cerca di ridurre il rischio di violazioni della sicurezza della postazione di lavoro. Lo scopo di questa politica è di prevenire eventi di data breach e responsabilizzare i dipendenti dell'Istituto. Di seguito sono elencati i comportamenti da applicare:

- i dipendenti sono tenuti a garantire che tutte le informazioni sensibili o confidenziali in formato elettronico o cartaceo siano messe al sicuro nella propria postazione di lavoro, in particolare alla fine della giornata lavorativa e in caso di assenza prolungata;
- i computer devono essere bloccati quando le postazioni di lavoro non sono occupate;
- tutti i computer devono essere spenti alla fine della giornata lavorativa;
- qualsiasi informazione e/o dato particolare/sensibile deve essere rimosso dalla scrivania e chiuso a chiave in un cassetto quando la postazione di lavoro non è occupata e alla fine della giornata lavorativa;
- le cartelle contenenti informazioni riservate e/o dati particolari/ sensibili devono essere tenute chiuse e bloccate quando non utilizzate;
- le chiavi utilizzate per accedere alle informazioni riservate e/o ai dati particolari/sensibili non devono essere lasciate su una scrivania non presidiata;
- i laptotp devono essere bloccati con un cavo di bloccaggio o conservati in un cassetto se non utilizzati;
- le password non possono essere lasciate su note adesive attaccate sopra o sotto un computer, né possono essere lasciate per iscritto su una postazione accessibile;
- le stampe contenenti informazioni riservate e/o dati particolari/sensibili devono essere immediatamente rimosse dalle stampanti;
- al momento dello smaltimento, i documenti riservati o contenenti dati particolari/sensibili devono essere triturati nei distruggidocumenti appositi;
- le lavagne contenenti informazioni riservate e/o dati particolari/sensibili devono essere cancellate;
- i dispositivi portatili come laptop, smartphone o tablet non devono mai essere lasciati sbloccati e incustoditi;
- tutti i dispositivi di archiviazione di massa come CDROM, DVD o chiavi USB contenenti informazioni riservate e/o dati particolari/sensibili devono essere conservati in cassetti chiusi a chiave.

Il dipendente che viola queste norme di comportamento può essere soggetto ad azioni disciplinari, fino al licenziamento.

### 7.4 Livelli di sicurezza, monitoraggio, revisione periodica

L'amministrazione della sicurezza logica segue i seguenti criteri generali:

- applicazione del principio "need to know" e del minimo privilegio, secondo cui la definizione dei profili standard da assegnare agli utenti con le autorizzazioni necessarie all'espletamento delle rispettive mansioni (definite per ruoli e competenze) avviene alla luce delle effettive esigenze operative. A tal scopo viene limitato l'accesso logico a reti, sistemi e basi dati;
- la validità delle richieste di accesso alla rete è verificata automaticamente dal sistema stesso prima di consentire l'accesso ai dati, tramite un sistema di autenticazione costituito da UserID e password;
- sono adottate delle indicazioni per la gestione delle password che indicano la lunghezza, la complessità, la durata, la conservazione sicura richiesta, nel caso di trattamenti dei dati effettuati con strumenti elettronici;
- sono previsti sistemi per la periodica validazione e il censimento delle utenze e delle abilitazioni;
- sono adottate tecniche e metodologie per la verifica nel continuo dell'utilizzo dei sistemi applicativi e per il controllo del traffico di rete generato, al fine di garantire pronto intervento in caso di attività anomale;
- sono previsti presidi rafforzati per l'accesso da remoto, in particolare nei confronti di utenti appartenenti a soggetti terzi;
- è prevista la revisione periodica delle misure di sicurezza, al fine di prevenire ipotesi di Data Breach;
- sono organizzate sessioni di formazione dei dipendenti, nonché regolamenti e altre forme di documentazione interna, al fine di rendere gli stessi edotti dei rischi in materia di privacy.
- Inoltre, vengono previsti periodici controlli al fine di verificare l'adeguatezza, l'affidabilità complessiva e la tutela del sistema informativo.

### 7.5 Amministratore di sistema

La figura professionale che, in ambito informatico, mantiene, configura e gestisce un sistema di elaborazione dati o sue componenti, ivi inclusi sistemi software complessi quali i sistemi Enterprise Resource Planning (system administrator), ovvero una base dati (database administrator), ovvero reti e apparati di telecomunicazione di sicurezza (network administrator) è nominata Amministratore di Sistema. L'attribuzione delle funzioni di Amministratore di sistema avviene previa valutazione delle caratteristiche di esperienza, capacità e affidabilità del soggetto designato, il quale fornisce idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di Trattamento, ivi compreso il profilo relativo alla sicurezza.

La nomina ad amministratore di sistema deve essere individuale, formalizzata, con l'indicazione analitica degli ambiti di applicazione di operatività consentiti in base al profilo di autorizzazione assegnato. In generale, l'Amministratore di sistema ha le seguenti responsabilità:

- sovraintendere alle risorse dei sistemi computerizzati al fine di consentirne una corretta ed efficiente utilizzazione;
- in accordo con il Manager della Protezione dei Dati personali, fornire guida e supporto agli Incaricati in merito al trattamento dei dati personali;

- amministrare e gestire la sicurezza informatica operando anche come gestore e custode delle password;
- nell'ambito delle responsabilità assegnate, effettuare periodici controlli e verifiche tecniche, anche nei riguardi degli Incaricati in merito a quanto previsto dal presente documento;
- individuare l'eventuale soggetto/i esterno/i quale manutentore del sistema stesso. L'amministratore che provvede alla designazione dei soggetti incaricati alla manutenzione deve preventivamente informare il Titolare del Trattamento e deve formalizzare per iscritto l'attribuzione dell'incarico eventualmente specificando i limiti dell'intervento e le manutenzioni richieste. Per manutenzione s'intende non soltanto l'intervento tecnico diretto ad eliminare eventuali avarie hardware, ma anche gli interventi volti alla ricostruzione di archivi che dovessero in qualche modo risultare danneggiati o corrotti oltre all'intervento tecnico diretto ad eliminare eventuali avarie al software di sistema e all'applicativo utilizzato;
- per poter svolgere funzioni, allo stesso vengono concesse dal Titolare le "Autorità di sistema", che consistono nell'assegnazione di attributi, privilegi, o accessi che consentono la gestione delle "risorse critiche del sistema operativo", ovvero degli oggetti informatici necessari al funzionamento dei sistemi e del servizio di elaborazione dati (es. log di sistema, tabella di servizio, cataloghi dei dati, ecc.).
- L'elenco dei soggetti nominati Amministratori di sistema sono conservati presso il Reparto IT e consegnati in copia per la custodia al Manager della Protezione dei dati.

## 8. Informazione e formazione del personale

L'obbiettivo di garantire un corretto trattamento dei dati, conforme ai requisiti previsti dalla normativa, viene raggiunto dalla Scuola anche e soprattutto grazie alla particolare attenzione risposta nei confronti della formazione del proprio personale.

A tal proposito, fin dal momento di ingresso di una nuova risorsa, ICS Arcisate presenta a quest'ultima la Policy Privacy, nonché le comunica eventuali aggiornamenti con e-mail inviata a tutti i dipendenti. Tale policy viene comunque archiviata all'interno della intranet dell'Istituto accessibile a tutti gli utenti di questa Istituzione scolastica.

Secondariamente, allo scopo di formare gli Incaricati dei trattamenti, la Scuola:

1. adotta un piano formativo con l'obiettivo di alfabetizzazione in materia di protezione dei dati personali, destinato a tutto il personale della Scuola;
2. prevede l'erogazione di un modulo relativo alla formazione privacy all'interno dei corsi organizzati all'atto dell'ingresso in servizio in questa Istituzione scolastica o anche al momento del cambio di mansione, qualora tale cambio preveda l'utilizzo di un nuovo applicativo, sistema o software all'interno della quale vengono trattati dati personali;
3. prevede un piano di formazione programmato con cadenza annuale sulla formazione erogata in ambito privacy a tutti i dipendenti della Scuola;
4. conserva la documentazione distribuita e la modulistica attestante la partecipazione agli interventi formativi.

La formazione degli incaricati riguarda in particolare:

- aspetti della disciplina di protezione dei dati personali, in ambito generale ed ambito specifico
- i rischi che minacciano i dati;
- le conseguenze derivate dalla violazione di dati personali (Data Breach);
- le procedure da seguire in caso di Data Breach;
- le misure disponibili per evitare eventi di Data Breach;
- aspetti della disciplina di protezione dei dati personali, in ambito generale ed ambito specifico;
- training per aggiornare il personale sulle misure adeguate di sicurezza e protezione dei dati personali adottate dal Titolare del trattamento;

La formazione deve essere:

- adeguata al proprio sistema di trattamenti dei dati;
- capace di trasmettere agli incaricati e responsabili del trattamento misure adeguate di sicurezza e protezione dei dati personali adottate dal Titolare;
- documentabile, in quanto la formazione dell'avvenuto training è parte integrante della policy privacy di questa Istituzione scolastica, e può essere richiesta in qualsiasi momento da enti specifici.

**Ministero dell'Istruzione, dell'Università e della Ricerca**

**ISTITUTO COMPRENSIVO STATALE DI SCUOLA DELL'INFANZIA, PRIMARIA E SECONDARIA DI PRIMO GRADO**

Via Lina Schwartz, 6 – 21051 ARCISATE (VA)

Tel: 0332 470122 - Fax: 0332 471854

codice ministeriale: vaic81800e – codice fiscale: 80018000127

sito internet: www.ics-arcisate.edu.it

email: vaic81800e@istruzione.it

email posta certificata: vaic81800e@pec.istruzione.it

Le seguenti istruzioni rivestono un ruolo fondamentale nell'attività dell'Istituto, perché rappresentano il modo con cui la Scuola si approccia ogni giorno al trattamento dei dati personali, considerandoli un valore da rispettare e proteggere, al di là degli obblighi che la legge ci impone.
Copie delle istruzioni sono distribuite a tutto il personale ed esposte in Istituto in modo da essere facilmente consultabili in ogni momento.

## Sommario

## *Principi applicabili al trattamento di dati personali*

Sono qui di seguito riportati in sintesi i principi del GDPR (art 5) che costituiscono il fondamento imprescindibile di tutti i trattamenti. Ogni soggetto che si trovi ad effettuare a qualsiasi titolo un trattamento di dati personali è tenuto alla stretta applicazione di queste prescrizioni;

a) Il trattamento di dati personali deve essere: LECITO, CORRETTO e TRASPARENTE
b) Le finalità del trattamento devono essere: DETERMINATE, ESPLICITE e LEGITTIME
c) I dati trattati devono essere ADEGUATI, PERTINENTI e LIMITATI allo stretto necessario
d) I dati trattati devono anche essere ESATTI e AGGIORNATI
e) I dati trattati devono essere CONSERVATI PER IL TEMPO STRETTAMENTE NECESSARIO a raggiungere le finalità
f) I dati vanno adeguatamente protetti da TRATTAMENTI NON AUTORIZZATI O ILLECITI e DALLA PERDITA, DALLA DISTRUZIONE O DAL DANNO ACCIDENTALI

## *Regolamento per l'utilizzo del sistema informatico*

### Premessa

La progressiva diffusione delle nuove tecnologie informatiche, ed in particolare il libero accesso alla rete Internet dai Personal Computer, espone l'Istituto ai rischi di un coinvolgimento sia patrimoniale sia penale, creando problemi alla sicurezza e all'immagine dello stesso.
Premesso quindi che l'utilizzo delle risorse informatiche e telematiche del nostro Istituto deve sempre ispirarsi a principi di diligenza e correttezza, comportamenti che normalmente si adottano nell'ambito di un rapporto di lavoro, viene adottato un Regolamento interno diretto ad evitare che comportamenti inconsapevoli possano innescare problemi o minacce alla Sicurezza nel trattamento dei dati.

**Utilizzo del Personal Computer**

Il Personal Computer affidato al dipendente è uno **strumento di lavoro**. Ogni utilizzo non inerente all'attività lavorativa può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza.
L'accesso all'elaboratore è protetto da password che deve essere custodita dall'incaricato con la massima diligenza e non divulgata.
Il custode delle parole chiave potrà accedere ai dati ed agli strumenti informatici esclusivamente per permettere alla stessa scuola, titolare del trattamento, di accedere ai dati trattati da ogni incaricato con le modalità fissate dalla stessa scuola, al solo fine di garantire l'operatività, la sicurezza del sistema ed il normale svolgimento dell'attività dell'Istituto nei casi in cui si renda indispensabile ed indifferibile l'intervento, ad esempio in caso di prolungata assenza od impedimento dell'incaricato, informando tempestivamente l'incaricato dell'intervento di accesso realizzato.
Non è consentito installare autonomamente programmi provenienti dall'esterno salvo previa autorizzazione esplicita del responsabile interno, in quanto sussiste il grave pericolo di portare Virus informatici e di alterare la stabilità delle applicazioni dell'elaboratore.
Non è consentito l'uso di programmi diversi da quelli distribuiti ed installati ufficialmente dall'Amministratore di Sistema. L'inosservanza di questa disposizione, infatti, oltre al rischio di danneggiamenti del sistema per incompatibilità con il software esistente, può esporre la scuola a gravi responsabilità civili ed anche penali in caso di violazione della normativa a tutela dei diritti d'autore che impone la presenza nel sistema di software regolarmente licenziato.

Non è consentito all'utente modificare le caratteristiche impostate sul proprio PC, salvo previa autorizzazione esplicita del responsabile interno.
Il Personal Computer deve essere spento ogni sera prima di lasciare gli uffici o in caso di assenze prolungate dall'ufficio. In ogni caso lasciare un elaboratore incustodito connesso alla rete può essere causa di utilizzo da parte di terzi senza che vi sia la possibilità di provarne in seguito l'indebito uso. In ogni caso deve essere attivato lo screen saver e la relativa password.
Non è consentita l'installazione sul proprio PC di nessun dispositivo di memorizzazione, comunicazione o altro (come ad esempio masterizzatori, modem, …), se non con l'autorizzazione espressa del responsabile interno.
Ogni utente deve prestare la massima attenzione ai supporti di origine esterna, avvertendo immediatamente il responsabile interno nel caso in cui vengano rilevati virus.

## Utilizzo della rete dell'Istituto

Le unità di rete sono aree di condivisione di informazioni strettamente professionali e non possono in alcun modo essere utilizzate per scopi diversi. Pertanto qualunque file che non sia legato all'attività lavorativa non può essere dislocato, nemmeno per brevi periodi, in queste unità. Su queste unità, vengono svolte regolari attività di controllo, amministrazione e backup.
Le password d'ingresso alla rete ed ai programmi sono segrete e vanno comunicate e gestite secondo le procedure impartite. È assolutamente proibito entrare nella rete e nei programmi con altri nomi utente.
Il responsabile interno può in qualunque momento procedere alla rimozione di ogni file o applicazione che riterrà essere pericolosi per la Sicurezza sia sui PC degli incaricati sia sulle unità di rete.
Costituisce buona regola la periodica (almeno ogni sei mesi) pulizia degli archivi, con cancellazione dei file obsoleti o inutili. Particolare attenzione deve essere prestata alla duplicazione dei dati. È infatti assolutamente da evitare un'archiviazione ridondante.
È cura dell'utente effettuare la stampa dei dati solo se strettamente necessaria e di ritirarla prontamente dai vassoi delle stampanti comuni. È buona regola evitare di stampare documenti o file non adatti (molto lunghi o non supportati, come ad esempio il formato pdf o file di contenuto grafico) su stampanti comuni. In caso di necessità la stampa in corso può essere cancellata.

## Gestione delle Password

Le password di ingresso alla rete, di accesso ai programmi e dello screen saver, sono previste ed attribuite dal responsabile interno. È necessario procedere alla modifica della password a cura dell'incaricato del trattamento al primo utilizzo e, successivamente, almeno ogni sei mesi; nel caso di trattamento di dati sensibili e di dati giudiziari la periodicità della variazione deve essere ridotta a tre mesi, con contestuale comunicazione al Custode delle Parole chiave.
Le password possono essere formate da lettere (maiuscole o minuscole) e numeri ricordando che lettere maiuscole e minuscole hanno significati diversi per il sistema; devono essere composte da almeno otto caratteri e non deve contenere riferimenti agevolmente riconducibili all'incaricato.
La password deve essere immediatamente sostituita, dandone comunicazione al Custode delle Parole chiave, nel caso si sospetti che la stessa abbia perso la segretezza.
Qualora l'utente venisse a conoscenza delle password di altro utente, è tenuto a darne immediata notizia alla Direzione o al responsabile interno.

## Utilizzo dei supporti magnetici

Tutti i supporti magnetici riutilizzabili (dischetti, cassette, cartucce) contenenti dati sensibili e giudiziari devono essere trattati con particolare cautela onde evitare che il loro contenuto possa essere recuperato. Una persona esperta potrebbe infatti recuperare i dati memorizzati anche dopo la loro cancellazione.
I supporti magnetici contenenti dati sensibili e giudiziari devono essere custoditi in archivi chiusi a chiave.

## Utilizzo di PC portatili

L'utente è responsabile del PC portatile assegnatogli e deve custodirlo con diligenza sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro.

Ai PC portatili si applicano le regole di utilizzo previste per i Pc connessi in rete, con particolare attenzione alla rimozione di eventuali file elaborati sullo stesso prima della riconsegna.

I PC portatili utilizzati all'esterno (convegni, visite in scuola, ecc…), in caso di allontanamento, devono essere custoditi in un luogo protetto.

## Uso della posta elettronica

La casella di posta, assegnata dalla scuola all'utente, è uno strumento di lavoro. Le persone assegnatarie delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse.

È fatto divieto di utilizzare le caselle di posta elettronica della scuola per l'invio di messaggi personali o per la partecipazione a dibattiti, forum o mail-list salvo diversa ed esplicita autorizzazione.

È buona norma evitare messaggi completamente estranei al rapporto di lavoro o alle relazioni tra colleghi. La casella di posta deve essere mantenuta in ordine, cancellando documenti inutili e soprattutto allegati ingombranti.

Ogni comunicazione inviata o ricevuta che abbia contenuti rilevanti o contenga impegni contrattuali o precontrattuali per la scuola deve essere visionata od autorizzata dalla Direzione, o in ogni modo è opportuno fare riferimento alle procedure in essere per la corrispondenza ordinaria.

La documentazione elettronica che costituisce per l'Istituto "know-how" aziendale tecnico o commerciale protetto e che, quindi, viene contraddistinta da diciture od avvertenze dirette ad evidenziarne il carattere riservato o segreto a tutela del patrimonio dell'impresa, non può essere comunicata all'esterno senza preventiva autorizzazione della Direzione.

È possibile utilizzare la ricevuta di ritorno per avere la conferma dell'avvenuta lettura del messaggio da parte del destinatario, ma di norma per la comunicazione ufficiale è obbligatorio avvalersi degli strumenti tradizionali (fax, posta, …).

Per la trasmissione di file all'interno della scuola è possibile utilizzare la posta elettronica, prestando attenzione alla dimensione degli allegati.

È obbligatorio controllare i file attachments di posta elettronica prima del loro utilizzo (non eseguire download di file eseguibili o documenti da siti Web o Ftp non conosciuti).

È vietato inviare catene telematiche (o di Sant'Antonio). Se si dovessero ricevere messaggi di tale tipo, si deve comunicarlo immediatamente al responsabile interno. Non si devono in alcun caso attivare gli allegati di tali messaggi.

## Uso della rete Internet e dei relativi servizi

Il PC abilitato alla navigazione in Internet costituisce uno strumento per la Scuola necessario allo svolgimento della propria attività. È assolutamente proibita la navigazione in Internet per motivi diversi da quelli strettamente legati all'attività lavorativa stessa.

È fatto divieto all'utente lo scarico di software gratuito (freeware) e shareware prelevato da siti Internet, se non espressamente autorizzato dal responsabile interno.

È tassativamente vietata l'effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti on-line e simili salvo i casi direttamente autorizzati dalla Direzione e con il rispetto delle normali procedure di acquisto.

È da evitare ogni forma di registrazione a siti i cui contenuti non siano legati all'attività lavorativa.

È vietata la partecipazione a Forum non professionali, l'utilizzo di chat line (esclusi gli strumenti autorizzati), di bacheche elettroniche e le registrazioni in guest books anche utilizzando pseudonimi (o nicknames).

## Osservanza delle disposizioni in materia di Privacy

È obbligatorio attenersi alle disposizioni in materia di Privacy e alle misure di sicurezza adottate dal Titolare del trattamento, come indicate nella lettera di designazione di incaricato del trattamento dei dati.

## Non osservanza della normativa dell'Istituto

Il mancato rispetto o la violazione delle regole contenute nel presente regolamento è perseguibile con provvedimenti disciplinari nonché con le azioni civili e penali consentite.

## Aggiornamento e revisione

Tutti gli utenti possono proporre, quando ritenuto necessario, integrazioni al presente Regolamento. Le proposte verranno esaminate dalla Direzione.
Il presente Regolamento è soggetto a revisione con frequenza annuale.

## *Regole pratiche per l'uso del PC di lavoro e del sistema informativo*

Tabella di facile consultazione per le principali cose da fare e non fare

| Comportamento corretto | Azioni da evitare |
|---|---|
| **PC di lavoro** | |
| Usare il proprio PC solamente per le finalità dell'Istituto<br>Avvertire subito in caso di anomalie<br>Spegnere il PC a fine giornata | Installare periferiche non fornite dalla scuola<br>Installare software non forniti dalla scuola<br>Caricare dati non forniti dalla scuola<br>Apportare modifiche alla configurazione |
| **Accesso al sistema informativo dell'Istituto** | |
| **Password personale** | |
| Modificare subito la password assegnata<br>Seguire le regole di seguito indicate per l'impostazione della password personale<br>Modificare la password ogni 3 o 6 mesi<br>Se esiste il dubbio che terzi siano venuti a conoscenza della password, informare subito il titolare | Comunicare la password solamente al custode delle password e solamente in forma segreta (cioè fornirgliene una copia senza che la possa conoscere) |
| **Accesso da PC diversi** | |
| | Accedere alle medesime applicazioni da PC diversi con lo stesso codice identificativo personale |
| **Antivirus** | |
| Procedere ai regolari aggiornamenti e procedere ad una scansione dopo ogni aggiornamento<br>Effettuare una scansione di qualsiasi supporto proveniente dall'esterno o destinato all'esterno della scuola, usando un antivirus aggiornato<br>Avvertire subito in caso di funzionamenti anomali | Usare qualsiasi supporto proveniente dall'esterno senza prima verificarne la sicurezza |
| **Copia dei dati** | |
| Copiare i dati ogni giorno<br>Usare più supporti a rotazione per la copia<br>Verificare periodicamente che il ripristino dai supporti sia corretto<br>Impedire che soggetti non autorizzati accedano ai supporti | Procedere alla copiatura senza autorizzazione<br>Utilizzare sempre lo stesso supporto<br>Tenere gli originali e le copie nello stesso posto |
| **Uso di supporti rimovibili** | |
| Applicare etichette sui supporti<br>Riutilizzare lo stesso supporto solo per lo stesso tipo di trattamento<br>Distruggere i supporti non più utilizzati<br>Rispettare le norme per la corretta distruzione dei supporti | Usare qualsiasi supporto per uso personale |
| **Aggiornamento dei sistemi** | |
| Seguire le indicazioni del titolare per l'aggiornamento di software, sistemi operativi, ecc. | Eseguire aggiornamenti di propria iniziativa |
| **Blocco della postazione** | |
| Impostare screen saver con password o altri sistemi analoghi per bloccare la postazione quando ci si allontana | |

| **File personali** | |
|---|---|
| | Utilizzarli in qualsiasi modo se non autorizzati |
| **Computer portatili e tablet** | |
| Crittografare i dati | Lasciare incustodito lo strumento |
| **Uso delle apparecchiature** | |
| Spegnere tutte gli strumenti elettronici al termine del loro utilizzo | |
| **Suggerimenti per la creazione delle password** | |
| Lunghezza della password: 8 caratteri minimo – 16 caratteri per utenti amministratori<br>Utilizzare lettere maiuscole e minuscole<br>Utilizzare lettere e numeri<br>Utilizzare anche caratteri non alfanumerici<br>Evitare riferimenti con la persona del relativo incaricato<br>Evitare di inserire parti del codice identificativo<br>Evitare l'utilizzo di parole di senso compiuto<br>Evitare sequenze di tasti vicini<br>Evitare di comunicarla a chicchessia<br>Evitare di scriverla in qualche posto<br>Evitare di digitarla in presenza di terze persone<br>Suggerimento: usare le iniziali delle parole che formano una frase che rappresenta un fatto di nostra conoscenza, per esempio: "quando sono andato a comprare il mio cane Boby pioveva che Dio la mandava". Ne risulta la psw: "qsaacimcBpcDlm", che possiamo ulteriormente complicare utilizzando simboli speciali: "$#qsaacimcBpcDlm#$" | |

## *Regole per la gestione dei documenti cartacei*

| Comportamento corretto | Azioni da evitare |
|---|---|
| **ACCESSO AI DOCUMENTI CARTACEI** | |
| Accedere, anche solo in consultazione, esclusivamente ai documenti per i quali si è stati espressamente autorizzati (ad esempio nella propria lettera d'incarico)<br>I documenti vanno prelevati dall'archivio e trattati in modo tale che terzi non autorizzati non possano accedervi<br>I documenti, al termine del trattamento o comunque al termine della giornata lavorativa, vanno riposti in archivio o nei propri cassetti opportunamente chiusi a chiave<br>I documenti con dati particolari (sensibili, giudiziari...) sono costantemente chiusi a chiave, salvo il tempo strettamente necessario al loro uso<br>Durante i trattamenti conservare i documenti in cartellette opache; nel caso di trattamenti dii dati sensibili o giudiziari o il cui trattamento presenta rischi specifici conservare i documenti in contenitori | Lasciare documenti incustoditi sulle scrivanie<br>Mostrare i documenti a terzi nono autorizzati<br>Portare fuori dalla scuola dati o documenti se non preventivamente autorizzati<br>Permettere l'accesso ai documenti, anche in sola consultazione, a terzi (ad esempio nei locali nei quali accedono persone esterne alla scuola)<br>Appendere documenti, o scrivere su lavagne, informazioni contenenti dati personali in locali accessibili a terzi |

| | |
|---|---|
| muniti di serratura<br>I documenti possono essere consegnati esclusivamente all'interessato al quale si riferiscono i dati | |
| **POSTAZIONE DI LAVORO** | |
| Riporre tutti i documenti prima di lasciare l'ufficio<br>Spegnere PC e periferiche non condivise al termine del lavoro | Lasciare incustoditi i documenti<br>Lasciare informazioni in vista sulla scrivania o sul PC |
| **FOTOCOPIATRICI** | |
| La copia va trattata come l'originale<br>Distruggere le copie non riuscite<br>Trasportare originale e copia con l'adeguata cura<br>Cancellare la memoria | Dimenticare l'originale<br>Fare copie inutili di documenti<br>Mostrare o distribuire copie a chi non è autorizzato al trattamento |
| **STAMPANTI** | |
| Distruggere le copie non riuscite<br>Cancellare la memoria | Dimenticare i documenti stampati<br>Fare copie inutili di documenti<br>Mostrare o distribuire stampe a chi non è autorizzato al trattamento |
| **RIFIUTI** | |
| Verificare che i documenti con dati personali non siano recuperabili, effettuandone una preventiva distruzione<br>Distruggere i supporti informatici e le apparecchiature in base alle disposizioni di legge | Gettare documenti o supporti leggibili se contengono dati personali o riservati |

## *Istruzioni per l'uso degli strumenti di comunicazione*

| Comportamento corretto | Azioni da evitare |
|---|---|
| **TELEFONO** | |
| Fornire solo le informazioni per le quali si è stati esplicitamente autorizzati<br>Segnalare al proprio responsabile richieste inusuali di informazioni<br>Nel caso di comunicazioni in viva voce informare l'interlocutore dell'attivazione di tale modalità e della presenza di eventuali altri ascoltatori; verificare in questo caso la presenza di terzi non autorizzati | Fornire informazioni sulle misure di sicurezza in atto<br>Fornire informazioni sull'organizzazione dell'Istituto<br>Fornire le proprie credenziali di autenticazione<br>Fornire informazioni relative agli interessati a terzi non autorizzati |
| **SEGRETERIE TELEFONICHE** | |
| | Lasciare informazioni riservate sulle segreterie telefoniche |
| **CELLULARI** | |
| Utilizzare password di accesso per la protezione della rubrica e dei dati<br>Bloccare il cellulare in caso di perdita o furto | Effettuare registrazioni audio, video o fotografiche mediante cellulari, palmari o altri dispositivi se non preventivamente autorizzati |

| | |
|---|---|
| **FAX IN USCITA**<br>(effettuabile solo da personale preventivamente autorizzato) | |
| Controllare il numero di telefono chiamato<br>Aggiungere avvertenza sulla riservatezza sui documenti inoltrati<br>Verificare il corretto inoltro<br>Cancellare la memoria | Dimenticare i documenti inoltrati e relativa ricevuta<br>EFFETTUARE INOLTRI AUTOMATIZZATI SENZA IL CONSENSO DEGLI INTERESSATI |
| **FAX/POSTA IN ENTRATA** | |
| Controllare il destinatario (scuola) prima di accedere ai documenti<br>Controllare il destinatario (interno) prima di accedere ai documenti<br>Cancellare la memoria | Accedere ai documenti che non ci sono indirizzati |
| **POSTA CONVENZIONALE IN USCITA**<br>(effettuabile solo da personale preventivamente autorizzato) | |
| Controllare che il destinatario sia corretto<br>Utilizzare una modalità di trasmissione congruente alla tipologia di trasmissione di dato (es. assicurata per dati sensibili) | |
| **POSTA ELETTRONICA**<br>(non fornisce garanzia di consegna al destinatario né di riservatezza del messaggio) | |
| L'uso dell'e-mail è limitato ai soggetti autorizzati<br>La posta elettronica è utilizzabile solo per fini istituzionali.<br>Nel caso di inoltro a più destinatari utilizzare come indirizzo di destinazione quello della scuola e mettere in CCN i singoli destinatari, per evitare che un destinatario possa conoscere l'indirizzo degli altri<br>Utilizzare un'adeguata dichiarazione di non-responsabilità in merito a privacy e riservatezza<br>L'invio di comunicazioni ufficiali o contenenti impegni contrattuali e precontrattuali deve essere autorizzata dal titolare | Utilizzare l'indirizzo dell'Istituto a fini personali<br>INOLTRARE IN AUTOMATICO E-MAIL SENZA IL CONSENSO DLL'INTERESSATO<br>Aprire e-mail e file provenienti da mittenti sconosciuti<br>Utilizzale l'e-mail per l'inoltro o la ricezione di dati sensibili, giudiziari o riservati<br>Inviare o memorizzare messaggi (interni ed esterni) di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica |
| **POSTA ELETTRONICA CERTIFICATA**<br>(effettuabile solo da personale preventivamente autorizzato)<br>La PEC ha lo stesso valore della raccomandata r.r. fra due caselle di PEC; il suo utilizzo deve sottostare alle medesime regole dll'Istituto che riguardano l'utilizzo della posta tradizionale. | |
| L'uso della PEC è limitato ai soggetti autorizzati<br>Verificare periodicamente la casella di PEC | |
| **CONVERSAZIONI** | |
| | Parlare con terzi o in luoghi pubblici o aperti al pubblico di fatti relativi all'attività dell'Istituto<br>Parlare anche con colleghi o in luoghi aziendali condivisi di informazioni alle quali tali colleghi non sono autorizzati ad accedere |
| **VISITATORI** | |

| | |
|---|---|
| Verificare l'identità<br>Invitare i visitatori a sostare nelle aree di attesa<br>Accompagnare i visitatori presso l'area di destinazione | Lasciare documenti visibili<br>Consentire l'accesso alle aree riservate<br>Consentire l'accesso a dati o documenti<br>Lasciare da solo un visitatore in un locale dove sono presenti documenti |
| **SALE RIUNIONI** | |
| | Lasciare materiale nelle sale riunioni |
| **CONVEGNI-PUBBLICAZIONI-SOCIAL NETWORK** | |
| | Dare informazioni sulla scuola e sulle attività della scuola senza la preventiva autorizzazione del titolare |

## *Istruzioni per la gestione dei supporti di memorizzazione*

| **Istruzioni per la gestione dei supporti di memorizzazione** | |
|---|---|
| Comportamento corretto | Azioni da evitare |
| Custodirli al fine di evitare accessi da parte di terzi non autorizzati<br>Custodirli adeguatamente durante il loro trasporto e la conservazione all'esterno della scuola<br>Distruggerli al termine della loro vita operativa<br>Distruggere i dischi fissi prima del loro smaltimento<br>Nel caso in cui, per motivi di manutenzione e riparazione, un elaboratore debba essere portato al di fuori della scuola, dovranno essere prese le opportune precauzioni affinchè terzi, non autorizzati, non possano accedere ai dati in esso contenuti | Esporli a fonti magnetiche o fonti di calore<br>Riutilizzarli per scopi diversi |
| Le corrette modalità di distruzione sono regolamentate dall'apposito provvedimento del Garante: **Rifiuti di apparecchiature elettriche ed elettroniche (Raae) e misure di sicurezza dei dati personali – 13 ottobre 2008**<br>*G.U. n.287 del 9 dicembre 2008* | |

## *Indicatori di un potenziale incidente informatico*

| **fenomeno riscontrato** | **probabile minaccia** |
|---|---|
| Rallentamento delle operazioni informatiche | adware<br>spyware |
| Rallentamento della navigazione | adware |
| Rallentamento delle comunicazioni | worm |
| Instabilità del computer | adware |
| Aperture anomale di pop-up | adware |
| Messaggi inconsueti e dal contenuto sospetto<br>Messaggi che chiedono la conferma o la modifica di credenziali<br>Messaggi che invitano a telefonare a un numero minacciando la sospensione di un servizio | Bluejacking<br>hoax<br>spam<br>spoofing<br>voice phishing |
| Anomalie di avvio del computer | vario tipo |
| Misterioso cambio della pagina iniziale del browser | dirottamento del browser |
| Apparizione di nuovi links nei “Preferiti” del browser | dirottamento del browser |
| Sparizione della voce “Opzioni” dal menu “Strumenti” del browser | dirottamento del browser |
| Difficoltà o impossibilità ad uscire da un sito web | mousetrapping |
| Reindirizzamenti non voluti a pagine web | page-jacking<br>pharming |
| Anomali messaggi di posta elettronica contenenti links | phishing |
| Applicazioni non desiderate | PUAs |
| Pop-up che invitano a scaricare un software “necessario” | spyware |
| E-mail con allegati eseguibili | Trojan |
| E-mail che iniziano con termini generici (es.“Gentile cliente”)<br>E-mail con dichiarazioni allarmanti<br>E-mail contenenti errori ortografici o caratteri strani | phishing |
| File con estensioni .exe, .com, .pif, .scr, .vbs, .shs, .chm e .bat o con doppia estensione (es. foryou.txt.vbs) | phishing |