PRIVACY	ISTITUTO COMPRENSIVO DI SAN MARTINO DI LUPARI
Documentazione redatta in ottemperanza a quanto disposto dal GDPR 2016/679 "*Regolamento generale sulla protezione dei dati*" e dalla normativa nazionale vigente	Scuola dell'Infanzia • Primaria • Secondaria di I grado VIA FIRENZE, 1 – 35018 SAN MARTINO DI LUPARI – PD Tel. 049 5952124 - www.icsanmartinodilupari.edu.it – C.F. 81001730282 Email PDIC838004@istruzione.it - Pec PDIC838004@pec.istruzione.it – Codice Univoco Ufficio UFYMWC

Disciplinare interno (di seguito Regolamento) per la sicurezza delle informazioni riservate e dei dati personali in responsabilità dell'Istituto.

Approvato nella seduta del XX Consiglio di Istituto del 3 aprile 2023 con delibera n. 149

Basi giuridiche:

- Regolamento in materia di Protezione dei Dati Personali (GDPR 2016/679 e D.Lgs. 196/2003 così come integrato dal D.Lgs. 101/18 e ss.mm.ii.);
- Statuto dei Lavoratori (Legge n. 300 del 1970, Legge delega n. 183 del 2014, D.Lgs. 15 giugno 2015, n. 81 e 14 settembre 2015, nn. 148, 149, 150 e 151, D.Lgs. 24 settembre 2016, n. 185);
- Circolare dell'Agenzia per l'Italia Digitale (AGID) n. 2 del 18 aprile 2017 relativa alle "Misure minime di sicurezza ICT per le pubbliche amministrazioni (Direttiva del Presidente del Consiglio dei ministri 01/08/2015);
- Linee Guida del Garante Privacy su Posta Elettronica e Internet (Deliberazione n. 13 del 01/03/2007 – G. U. n. 58 del 10/03/2007);
- Decreto ministeriale 7 dicembre 2006 n. 305 Regolamento recante identificazione dei dati sensibili e giudiziari trattati e delle relative operazioni effettuate dal Ministero della pubblica istruzione, in attuazione degli articoli 20 e 21 del decreto legislativo 30 giugno 2003, n. 196, recante "Codice in materia di protezione dei dati personali" (G.U. n. 11, 15 gennaio 2007, Serie Generale);
- Codice Amministrazione Digitale (CAD): D.Lgs. 7 marzo 2005, n. 82, modificato e integrato dal D.Lgs. 22 agosto 2016 n. 179 e dal D.Lgs. 13 dicembre 2017 n. 217;
- LEGGE 9 gennaio 2004, n. 4 Disposizioni per favorire e semplificare l'accesso degli utenti e, in particolare, delle persone con disabilità agli strumenti informatici (Regolamento 01/02/2004 pubblicato il 14/09/2020);
- L. 633/41 Protezione del diritto d'autore e di altri diritti connessi al suo esercizio, D.Lgs 68/2003 sulla regolamentazione per la tutela del diritto d'autore e dei diritti connessi nella società dell'informazione, L. 248/2000 nuove norme di tutela del diritto d'autore;
- D.P.R. n. 275/99 Regolamento recante norme in materia di autonomia delle istituzioni scolastiche, ai sensi dell'art. 21 della legge 15 marzo 1997, n. 59;
- L. 547/1993 Norme in materia di reati informatici;
- Decreto legislativo, 23/06/2003 n° 195, G.U. 29/06/2007;
- Circolare INL n. 2 del 2016;
- D. Lgs. 518/92 sulla tutela giuridica del software;
- L. 18 48/08 Ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica, fatta a Budapest il 23 novembre 2001, e norme di adeguamento interno;
- Articolo 612 ter, 615 bis, 615 ter, 615 quater, 615 quinquies, 616, 617, 617 bis, 617 ter, 617 quater, 617 quinquies, 617 sexies, 618, 619, 620, 623 bis del C.P.;
- Provvedimento del Garante per la protezione dei dati personali n. 13 del 1° marzo 2007;
- Provvedimento del Garante per la protezione dei dati personali n. 139 del 2018;
- Provvedimento del Garante per la protezione dei dati personali del 27/11/2008 poi modificato il 26 giugno 2009 (c.d. Provvedimento sugli Amministratori di Sistema);
- Provvedimento del Garante per la protezione dei dati personali del 13 ottobre 2008.

Anche nel rispetto delle disposizioni previste dalle Regole tecniche in materia di conservazione digitale degli atti definite da AGID, dei tempi e dei modi indicati dalle "Linee guida per gli archivi delle istituzioni scolastiche" e dal "Piano di conservazione e scarto per gli archivi delle Istituzioni scolastiche", redatti dal Ministero per i Beni e le attività Culturali - Direzione Generale per gli Archivi.

LEGENDA:

- **Utenti interni e/o esterni**: per utenti interni si intendono gli studenti iscritti che possono utilizzare, per scopi didattici, gli strumenti informatici dell'Istituto. Per utenti esterni si intendono le persone fisiche, le aziende private, le altre pubbliche amministrazioni che, sulla base di rapporti contrattuali o convenzionali autorizzati preventivamente dall'Istituto, accedono dall'esterno del sistema informatico scolastico;
- **Incaricati (autorizzati) al trattamento**: persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile.

Entrata in vigore del Regolamento
Con l'entrata in vigore del presente regolamento tutte le disposizioni in precedenza adottate in materia, in qualsiasi forma comunicate, devono intendersi abrogate e sostituite dalla presente.

Parte prima: utilizzo degli strumenti informatici, posta elettronica e internet dell'Istituto

In questa parte si adottano, nel rispetto delle normativa vigente, i comportamenti necessari per definire la gestione e l'utilizzo delle risorse informatiche interne, in sinergia con le necessarie attività istituzionali, al fine di evitare che un utilizzo non adeguato dei predetti strumenti possa comportare una violazione dei dati personali, o la compromissione, in tutto e/o in parte, dell'infrastruttura informatica.
E' dovere dell'Amministrazione fornire un'adeguata informazione circa le modalità e i doveri che ciascuno deve osservare per il corretto uso delle predette risorse, durante lo svolgimento delle mansioni lavorative o durante la partecipazione attiva alle varie attività istituzionali. Questo anche per sviluppare la necessaria sensibilizzazione sul valore della sicurezza del patrimonio informatico e sulla tutela dei diritti e delle libertà degli interessati, previsti dalla normativa sulla protezione dei dati personali.

INTRODUZIONE

La progressiva diffusione delle nuove tecnologie informatiche, ed il libero accesso alla rete Internet, espone **l'Istituto Comprensivo di San Martino di Lupari** a potenziali rischi in termini di sicurezza informatica con possibili conseguenze patrimoniali, penali e di immagine dell'Istituto stesso.
Premesso quindi, che l'utilizzo delle risorse istituzionali deve sempre ispirarsi al principio della diligenza e della correttezza, l'Istituto adotta il seguente Regolamento, che integra le disposizioni di cui agli artt. 2104 e 2105 codice civile, quelle dei CCNL e delle procedure e degli altri regolamenti adottati in Istituto.
Alle prescrizioni di seguito previste si aggiungono ed integrano inoltre le specifiche istruzioni già fornite a tutti gli incaricati (soggetti designati ex art. 2-quaterdecies D.Lgs 101/2018 ed incaricati ex art. 29 del GDPR 2016/679) ed utenti (studenti e famiglie, consulenti collaboratori esterni pubblici e privati), in attuazione del GDPR 2016/679 e dalla normativa nazionale vigente.
Considerato inoltre che l'Istituto, nell'ottica di uno svolgimento proficuo e più agevole della propria attività, potrebbe decidere di mettere a disposizione dei propri dipendenti in caso di necessità, adeguate risorse informatiche (computer portatili, telefoni cellulari, tablet, etc.), sono state inserite nel regolamento alcune clausole relative alle modalità ed i doveri che ciascun dipendente deve osservare nell'utilizzo di tale strumentazione.

OBBLIGHI

Ogni utente è responsabile civilmente e penalmente del corretto uso delle risorse informatiche, dei servizi/programmi ai quali ha accesso e dei dati personali propri o trattati per conto dei diretti interessati. Tutti i soggetti che interagiscono, a qualunque titolo, col sistema informatico dell'Istituto sono anche responsabili degli eventuali danni erariali conseguenti.

INCARICATI

In capo al personale dipendente vige l'obbligo di adottare comportamenti preventivi, conformi al corretto espletamento della prestazione lavorativa, che impediscano il verificarsi di situazioni di rischio negli strumenti affidati e nei relativi dati personali contenuti.
In particolar modo, questo principio universale vale anche nel caso in cui sia previsto l'uso a fini privati dei dispositivi informatici di proprietà dell'Istituto. Questa specifica modalità d'uso deve essere però tassativamente autorizzata dal presente Regolamento o da altri testi attuativi adottati dall'amministrazione che contengano ulteriori norme circa le procedure organizzative e gestionali in responsabilità dell'Istituto. In difetto deve ritenersi vietata.

UTENTI INTERNI ED ESTERNI

Il curriculum scolastico prevede espressamente che gli studenti imparino ad utilizzare gli strumenti informatici per favorire la formazione tecnologica delle competenze, la promozione della cultura, l'innovazione, la condivisione delle conoscenze e delle esperienze. L'accesso alle risorse informatiche dell'Istituto costituisce pertanto un diritto che prevede delle responsabilità in capo all'utilizzatore, o su chi esercita su quest'ultimo la responsabilità genitoriale (in caso di studenti minori). Gli studenti pertanto sono tenuti ad usare queste risorse in modo corretto e responsabile, impegnandosi ad utilizzare il servizio erogato dall'Istituto nel pieno rispetto della legislazione vigente e degli altri regolamenti interni previsti (vedasi ad esempio il "REGOLAMENTO UTILIZZO PIATTAFORME PER LA DIDATTICA A DISTANZA" , REGOLAMENTO DDI , / REGOLAMENTO-PER-LA-

PREVENZIONE-DI-BULLISMO-E-CYBERBULLISMO), limitando le attività esclusivamente per scopi didattici e/o istituzionali. Eventuali violazioni saranno perseguite, ove previsto, in base a quanto disposto nello specifico regolamento sul Cyberbullismo, fermo restando ulteriori azioni che l'Istituto potrà intraprendere presso le sedi competenti.

Anche in capo agli utenti esterni (fra i quali rientrano anche i cosiddetti Responsabili esterni di cui all'art. 28 comma 1 del GDPR 2016/679, gli stagisti curriculari, i formatori, gli enti convenzionati, ecc.) che accedono all'infrastruttura informatica dell'Istituto, limitatamente alle sole attività preventivate e contrattualizzate, valgono le stesse indicazioni riportate nel paragrafo 'OBBLIGHI' di cui sopra.

CAMPO DI APPLICAZIONE

All'interno del presente documento non sempre è possibile fornire indicazioni puntuali sulla totalità degli strumenti informatici dell'Istituto in quanto risulterebbe difficile contemplare ogni tipologia di dispositivo informatico e di informazione di interesse istituzionale. Risulta per tale ragione fondamentale comprendere la logica alla base e le finalità del presente documento, per poter seguire in modo efficace le indicazioni fornite, nel pieno rispetto delle leggi vigenti.

NORME COMPORTAMENTALI (INCARICATI)

Norme tecniche
Chiunque utilizzi gli strumenti informatici dell'Istituto è tenuto a prendere visione e ad attenersi a quanto previsto nel presente Regolamento.

- Il personale che tratta dati personali è tenuto al rispetto e alla cura, secondo la diligenza del buon padre di famiglia, di tutte le apparecchiature messe a disposizione dall'Istituto, provvedendo alla buona conservazione delle stesse, verificando, al termine dell'orario di lavoro, di lasciare la propria postazione ordinata, con le apparecchiature debitamente spente (salvo indicazioni contrarie da parte del Responsabile IT o della Direzione) e libera da documenti che possano implicare il trattamento, da parte di terzi non autorizzati, di informazioni riservate e/o dati personali.
- Al momento di lasciare incustoditi i locali e/o gli uffici, il personale dovrà altresì accertarsi della chiusura di finestre, di porte e di tutti gli arredi che contengono dati personali e/o riservati, nonché di non lasciare attiva la sessione di lavoro nei dispositivi informatici.
- **E' assolutamente vietato lasciare incustodite o non adeguatamente protette le proprie credenziali, relative a computer/servizi/portali della scuola, accessibili a terzi, interni e/o esterni (es: post-it, appunti sul planning, file privi di protezione in cartelle condivise, agende o block-notes).**
- E' assolutamente vietato memorizzare le proprie credenziali, relative ai computer/servizi/portali della scuola, nei browser dei dispositivi informatici.
- I personal computer forniti dall'Istituto ed eventuali dispositivi mobili, utilizzati dal personale, sono sempre considerati strumenti di lavoro. Ogni utilizzo improprio può causare disservizi, ulteriori costi di manutenzione e soprattutto minacce alla sicurezza, alla protezione dei dati personali in essi contenuti, nonché alle informazioni costituenti patrimonio dell'Amministrazione. Nei personal computer forniti dall'Amministrazione è vietato l'inserimento di dispositivi di memoria (supporti magnetici o ottici, CD-ROM, DVD–ROM, Pen Drive, HDD esterni, ecc.) a meno che non siano stati preventivamente autorizzati dalla Direzione, anche a mezzo di integrazione specifica del presente Regolamento.
- Fatta eccezione per i dispositivi presenti nella segreteria scolastica, le informazioni riservate e/o le particolari categorie di dati personali (c.d. sensibili) potranno essere conservate nei computer della scuola (limitatamente alla sola aula insegnanti) solo per il tempo strettamente necessario all'evasione del servizio (mera creazione e successivo completamento del documento), solo se adeguatamente e preventivamente protette (es.: cifratura tramite protezione con password adeguata). E' invece fatto assoluto divieto di conservare, all'interno degli ulteriori dispositivi informatici della didattica (laboratori informatici, aule didattiche, aule di sostegno, ecc.), qualsiasi documento che contenga informazioni riservate e/o le particolari categorie di dati personali (c.d. sensibili);
- Il personale non deve modificare la configurazione del proprio personal computer. In caso di mal funzionamento, se non si possiedono le informazioni tecniche ed organizzative necessarie a risolvere in autonomia il problema, si dovrà richiedere l'intervento dei soli tecnici preposti.
- E' fatto divieto di installare nelle apparecchiature software provenienti da fonti non verificate e comunque non preventivamente autorizzati dalla Direzione. Si ricorda in particolare che il mancato rispetto delle norme relative alle licenze d'uso è perseguibile penalmente.
- E' assolutamente vietato modificare i dati contenuti nei programmi gestionali salvo quelli esplicitamente autorizzati nel profilo di lavoro personale, ed è altresì vietato effettuare modifiche, attraverso gli strumenti di sviluppo, di qualsivoglia componente del programma stesso.

- Tutta la documentazione prodotta dal personale incaricato al trattamento dovrà essere elaborata esclusivamente con gli strumenti messi a disposizione dall'Istituto, a meno che non siano stati preventivamente autorizzati strumenti alternativi dalla Direzione, anche a mezzo di integrazione specifica del presente Regolamento, e dovrà essere inserita negli archivi autorizzati.
- Nei dispositivi informatici di proprietà dell'Istituto sarà effettuato periodicamente un controllo dei supporti di memoria (es. dischi fissi), al fine di verificarne l'efficienza e per provvedere all'eventuale eliminazione dei file obsoleti e/o non pertinenti, escludendo a priori l'accesso ai relativi contenuti.
- È fatto divieto di memorizzare, salvare file e/o cartelle non pertinenti al contesto lavorativo, didattico ed istituzionale o in posizioni non autorizzate, anche in cloud.
- Dovrà essere previsto il salvataggio nel server dell'Istituto di tutti i documenti informatici contenenti dati personali ove l'infrastruttura tecnologica dell'Istituto lo consenta. Non è consentita la memorizzazione di questi documenti sui singoli dischi locali dei dispositivi (se non temporaneamente ove previsto nel presente Regolamento).
- Poiché i "malware" (virus, worm, spyware e altri programmi dannosi con lo scopo di causare danni al sistema su cui vengono eseguiti) costituiscono una delle minacce più frequenti alla sicurezza, è necessario che il personale incaricato al trattamento si attenga alle seguenti norme:
  - il sistema informatico dispone di software di protezione aggiornato automaticamente (es. antivirus); si raccomanda pertanto di verificarne periodicamente l'effettivo funzionamento (ad esempio, controllare eventuali segnalazione di errore come punti esclamativi sull'icona del programma dell'antivirus, nel menu posto in basso a destra della barra delle applicazioni) e di non disattivare mai tali software di protezione per alcun motivo;
  - è vietato utilizzare qualsiasi materiale che potrebbe contenere virus o altri software dannosi (allegati a mail non verificate, software di cui non si conosca la provenienza o l'autenticità, software presente su supporti esterni, anche se personali, sui cui non sia stato svolto un preventivo controllo da eventuali minacce, ecc.).

NORME COMPORTAMENTALI (UTENTI INTERNI)

Norme tecniche
Chiunque utilizzi gli strumenti informatici dell'Istituto è tenuto a prendere visione e ad attenersi a quanto previsto nel presente Regolamento.

- **Lo studente** è tenuto al rispetto e alla cura di tutte le apparecchiature messe a disposizione dall'Istituto, provvedendo alla buona conservazione delle stesse, verificando di lasciare la propria postazione ordinata e con le apparecchiature debitamente spente al termine della propria sessione di studio, salvo indicazioni contrarie da parte dei docenti.
- I personal computer forniti dall'Istituto ed eventuali dispositivi mobili, utilizzati dagli studenti, sono strumenti didattici. Ogni utilizzo improprio può causare disservizi, ulteriori costi di manutenzione e soprattutto minacce alla sicurezza, alla protezione dei dati personali in essi contenuti, nonché alle informazioni costituenti patrimonio dell'Amministrazione. Nei personal computer forniti è vietato l'inserimento di dispositivi di memoria (supporti magnetici o ottici, CD-ROM, DVD–ROM, Pen Drive, HDD esterni, ecc.) a meno che non siano stati espressamente autorizzati o verificati dal Docente. La responsabilità dei contenuti nei dispositivi di memoria, ove consentiti, resta comunque a totale carico dei rispettivi proprietari o di chi ne esercita la responsabilità genitoriale (nel caso di studenti minori).
- Lo studente non deve modificare la configurazione del personal computer a cui viene assegnato; in caso di mal funzionamento dovrà segnalare l'accaduto ai docenti che avranno cura di richiedere l'intervento dei soli tecnici preposti. Si fa inoltre divieto di installare nelle apparecchiature software non autorizzati dal Docente o dalla Direzione. Si ricorda che il mancato rispetto delle norme relative alle licenze d'uso è perseguibile penalmente.
- Nei dispositivi informatici di proprietà dell'Istituto sarà effettuato periodicamente un controllo dei supporti di memoria (es. dischi fissi), al fine di verificarne l'efficienza e per provvedere all'eventuale eliminazione dei file obsoleti e/o non pertinenti, escludendo a priori l'accesso ai relativi contenuti.
- È fatto divieto di salvare file e/o cartelle non pertinenti con il contesto didattico ed istituzionale o in posizioni non autorizzate, anche in cloud.
- Non è consentita la memorizzazione di documenti informatici, contenenti dati personali, nei singoli dischi locali dei dispositivi (se non temporaneamente ove previsto nel presente Regolamento).
- Poiché i "malware" (virus, worm, spyware e altri programmi dannosi con lo scopo di causare danni al sistema su cui vengono eseguiti) costituiscono una delle minacce più frequenti alla sicurezza, è necessario che anche gli studenti si attengano alle seguenti norme:
  - il sistema informatico dispone di software di protezione aggiornato automaticamente (es. antivirus); si raccomanda pertanto di non disattivare mai i software di protezione per alcun motivo.
  - è vietato utilizzare qualsiasi materiale che potrebbe contenere virus o altri software dannosi (allegati a mail non verificate, software di cui non si conosca la provenienza o l'autenticità, software presente su supporti esterni, anche se personali, sui cui non sia stato svolto un preventivo controllo da eventuali minacce, ecc.).

NORME COMPORTAMENTALI (UTENTI ESTERNI)

Anche per i visitatori (fornitori, formatori, stagisti, collaboratori della scuola per attività formative o di segreteria) valgono le stesse indicazioni previste per gli studenti (Utenti Interni), fermo restando che, nel caso di utilizzo degli strumenti informatici dell'Istituto, da parte di soggetti esterni, questi dovranno prevedere obbligatoriamente la creazione di account specifici.
In ogni caso tali situazioni specifiche andranno disciplinate nel dettaglio, con apposito regolamento.

SISTEMI INFORMATIVI

GESTIONE DELLE PASSWORD

L'accesso ad ogni postazione di lavoro individuale, alla rete e alle applicazioni aziendali avviene mediante password personali. Le password sono utilizzate per accedere a differenti profili di autorizzazione nell'ambito del sistema informativo aziendale (es. utenze contabilità aziendale, accesso ad Internet, sistemi di posta elettronica, ecc.).

Parole chiave deboli

Le password di facile individuazione hanno le seguenti caratteristiche:
- Si possono trovare in un comune dizionario italiano, inglese o altra lingua comune;
- Sono parole di uso comune legate all'utente (nome di qualche membro della famiglia, di animali domestici, di amici, di collaboratori, ecc.);
- Sono legate ad informazioni personali (date di nascita, indirizzi, numeri telefonici, ecc.);
- Sono legate ad espressioni informatiche, hardware e software;
- Sono sequenze ripetute del tipo "11111111", "22222222", "12121212", "12345678", pass-1234, ecc.
- Sono considerate "deboli" anche le parole chiave precedentemente indicate, precedute o seguite da una cifra (giovanni1, 1giovanni, ecc.).

Parole chiave sicure

Sono da ritenere password di soddisfacente sicurezza quelle che hanno le seguenti caratteristiche: sono **composte da caratteri maiuscoli e minuscoli, utilizzano anche caratteri di interpunzione, come [ ] ! ? * " , ; ed una miscela di numeri e lettere**.

Un altro importante accorgimento riguarda la selezione di parole chiave, che possano essere facilmente digitate sulla tastiera, senza doverla guardare, per ridurre al minimo il tempo di digitazione ed evitare che la digitazione possa essere osservata da terzi nelle vicinanze.

NOTA: Le password non devono mai essere scritte su documenti cartacei accessibili, post-it o archiviate in linea sui sistemi aziendali (banche dati o postazioni di lavoro). Inoltre non devono essere conservate, facilmente accessibili, nell'ambito della propria postazione di lavoro o, peggio, sugli strumenti informatici in dotazione.

SALVA SCHERMO

I dispositivi sono protetti da una impostazione del sistema operativo che, dopo un determinato periodo di inattività dell'elaboratore, attiva uno "screen saver" (o salvaschermo) sbloccabile solo con password. Il personale è tenuto a bloccare, in ogni caso, il proprio computer (fisso o laptop) nel momento in cui si allontana da esso anche per periodi più brevi (ad esempio attivando manualmente il blocca schermo, tramite disconnessione dell'utente). Qualora la modalità di blocco non fosse presente, il personale è tenuto ad informare tempestivamente i tecnici incaricati, il Responsabile IT e/o la Direzione.

DISCHI DI RETE

L'Istituto dispone dei cosiddetti 'Dischi di Rete'. Si tratta di spazi di memorizzazione creati su dispositivi dedicati che permettono di memorizzare e condividere dati attraverso la rete, e che vengono protetti con sistemi avanzati di backup. Questa misura garantisce la disponibilità del dato in caso di perdita o malfunzionamento dei dispositivi di memorizzazione.
I file che vengono prodotti in locale, qualora non sia già presente un automatismo previsto dai tecnici incaricati e/o dall'Responsabile IT, devono essere salvati sempre anche nel disco di rete e, una volta che non sussistano più ragioni di convenienza, i file locali

devono essere eliminati a favore della sola conservazione sul disco di rete. Le cartelle nei dischi di rete possono essere create per area, per competenza o per singolo utente (vedere anche il punto successivo per la cartella personale nei dischi di rete).
Le password d'accesso alla rete, ai relativi dischi ed ai programmi sono segrete e vanno comunicate e gestite secondo le procedure previste. È assolutamente proibito autenticarsi nella rete e nei programmi con altri nomi utente.

CARTELLE PERSONALI

Nei dischi di rete possono essere presenti cartelle (per area o nominative) per il salvataggio dei propri dati. In tali cartelle devono essere salvati tutti i file di cui l'Istituto ha un preciso obbligo di conservazione, anche se memorizzati temporaneamente in locale su personal computer.
In caso di furto o smarrimento dei dispositivi, infatti, la copia "in rete" garantirà la disponibilità delle informazioni. Si ribadisce che il personale non deve mantenere informazioni o dati personali, in responsabilità all'Istituto, nel proprio disco locale, ma utilizzare i dischi di rete o le piattaforme digitali online, con le modalità indicate nel presente Regolamento, autorizzate dall'Istituto, al fine di garantirne la disponibilità e la riservatezza in caso di eventi dannosi.
Non è ammessa l'archiviazione in locale di file con dati personali, qualora non sia prevista la possibilità di creare una copia di sicurezza anche nei dischi di rete.

SUPPORTI E SERVIZI DI MEMORIZZAZIONE

E' vietato trattare dati personali su supporti di memorizzazione fisici (HDD esterni, Pendrive, CD/DVD/R/RW, ecc.) o virtuali (Cloud) al di fuori delle indicazioni previste nel presente regolamento senza che le informazioni non siano adeguatamente e preventivamente protette (es.: cifratura tramite protezione con password adeguata) e senza che tali attività siano autorizzate dalla Direzione.
Si ricorda che è necessario eliminare sempre i dati personali dai supporti di memorizzazione in maniera sicura, in modo che le informazioni non risultino accessibili. Nel caso in cui non si disponga delle informazioni tecniche necessarie a tali scopi si dovrà interpellare l'Responsabile IT o i tecnici incaricati.

UTILIZZO DI DISPOSITIVI MOBILI

Per dispositivo mobile si intendono tutti quei dispositivi informatici che sono utilizzabili seguendo la mobilità dell'utente, quali telefoni cellulari, palmari, smartphone, tablet, laptop, ecc. Il termine designa in modo generico le tecnologie di elaborazione o accesso ai dati (anche via Internet) prive di vincoli sulla posizione fisica dell'utente o delle apparecchiature coinvolte.

DISPOSITIVI MOBILI

DI PROPRIETÀ DELL'ISTITUTO (UTENTI INTERNI E INCARICATI)

Nel caso in cui si dovessero assegnare dispositivi mobili ad utenti ed incaricati, essi sono assegnati individualmente. Gli utenti interni e gli incaricati rispondono del loro utilizzo e devono custodirli con diligenza, sia durante gli spostamenti, sia durante l'eventuale utilizzo intra ed extra Istituto, previa sottoscrizione di specifico **contratto di comodato d'uso**, da reperirsi presso la segreteria dell'Istituto.
Ai dispositivi mobili concessi in uso dall'Istituto si applicano le stesse regole di utilizzo previste per i computer connessi in rete, con particolare attenzione alla rimozione di eventuali file elaborati sullo stesso, prima della riconsegna.
Non è consentito l'uso di qualsiasi dispositivo esterno collegabile al dispositivo mobile, se non quelli istituzionali o quelli autorizzati.
L'utilizzatore che abbia necessità di apportare modifiche hardware o software al dispositivo mobile in dotazione, deve farne preventiva richiesta alla Direzione o al Responsabile IT.
Quanto memorizzato sui supporti interni al dispositivo mobile potrebbe essere oggetto di analisi, controllo e duplicazione da parte del Responsabile IT o da personale tecnico autorizzato, per migliorare l'affidabilità, la disponibilità, l'efficienza del dispositivo.
Qualora fossero individuate componenti hardware e/o software (programmi, documenti, dispositivi esterni, ecc.) non corrispondenti ai criteri di sicurezza e di operatività individuati dal Responsabile IT o non esplicitamente e preventivamente autorizzati, tali componenti potranno essere rimossi.

Disposizioni operative per l'utilizzo dei dispositivi mobili

- E' espressamente vietato conservare dati personali all'interno del dispositivo mobile senza adottare preventivamente adeguate misure di sicurezza (es.: cifratura tramite protezione con password adeguata).
- I dispositivi mobili devono avere abilitato il codice di blocco e/o il PIN d'accesso e/o la Password personalizzata. Tale codice d'accesso dev'essere impostato con almeno 8 caratteri alfanumerici (o, nei casi in cui non sia possibile, al massimo del numero di caratteri consentiti dallo strumento), deve essere complessa (lettere maiuscole e minuscole, numeri e caratteri speciali), non deve richiamare né date di nascita né altri riferimenti anagrafici. La password individuata dovrà essere comunicata al Responsabile IT o alla Direzione, sia al primo uso sia quando modificata alle scadenze prefissate.
- E' fatto espresso divieto di memorizzare nel dispositivo mobile qualsiasi credenziale che permetta l'accesso ad aree riservate in responsabilità all'Istituto.
- E' fatto espresso divieto di utilizzare qualsiasi dispositivo mobile istituzionale durante la guida. L'uso in auto è consentito, ove previsto, solo mediante kit "viva voce" e/o con auricolare.
- Nel caso di dispositivi di proprietà dell'Istituto è vietato utilizzare qualsiasi software e/o tecnica di jailbreack (Apple) o root (Android), che consentono di abilitare l'utente amministratore ed avere accesso al kernel o nucleo del sistema operativo ed a tutti i file di sistema.
- Sugli strumenti in dotazione forniti dall'Istituto possono essere utilizzati solamente software forniti o autorizzati dall'Istituto; pertanto non si possono acquisire e installare autonomamente software e applicazioni, senza una specifica verifica e autorizzazione da parte del Responsabile IT e della Direzione. E' vietato utilizzare software senza licenza d'uso (D.Lgs. 518/92 sulla tutela giuridica del software e L. 248/2000 sulle nuove norme di tutela del diritto d'autore).
- I dispositivi mobili devono essere dotati di software di '*remote wiping*' che permettano la cancellazione dei contenuti da remoto, una volta che il dispositivo dovesse essere oggetto di furto o smarrimento. Se l'installazione di questo software non fosse stata predisposta, l'utilizzatore dovrà informarne tempestivamente il Responsabile IT o la Direzione.
- I dispositivi mobili devono essere dotati di software antivirus aggiornabile automaticamente e con la funzione di monitoraggio attiva. Se l'installazione di questo software non fosse stata predisposta, l'utilizzatore dovrà informarne tempestivamente il Responsabile IT o la Direzione.
- Non è consentito all'utilizzatore disattivare l'antivirus, in tutto o in parte.
- Se il dispositivo mobile consente l'attivazione dei servizi di tethering, ovvero consente la configurazione dell'apparato come "gateway" per condividere l'accesso alla Rete Internet per altri dispositivi che ne sono sprovvisti, questo tipo di possibilità va usata solo per periodi molto limitati e solo in assenza di ogni altra soluzione di connettività fornita dall'Istituto. Il servizio va immediatamente disattivato al termine dell'utilizzo e va protetto da password adeguata come previsto nei punti precedenti.
- L'eventuale periferica WiFi va abilitata sul dispositivo mobile ai fini d'accesso alla rete istituzionale e/o ad altre reti protette, e mai pubbliche, e solo ed esclusivamente per il tempo necessario a tali attività.
- Il Bluetooth ed ogni altro protocollo che consenta l'associazione di dispositivi diversi dallo strumento mobile, dev'essere abilitato per l'accoppiamento ai soli strumenti istituzionali in dotazione. Può essere liberamente usato per l'attivazione dell'auricolare personale e/o del kit viva-voce dell'auto. Il Bluetooth non va mai lasciato inutilmente attivo e le password d'associazione non devono mai essere quelle di default previste per il dispositivo.

PRIVATI: NOTEBOOK (UTENTI INTERNI E INCARICATI)

E' fatto espresso divieto di conservare nei dispositivi mobili privati qualsiasi dato personale e/o informazione riservata in responsabilità dell'Istituto senza adottare preventivamente adeguate misure di sicurezza (es.: cifratura dei file tramite protezione con password adeguata, criptazione delle unità di memoria, impostazione di servizi di wiping del device).
Il contenuto dei dispositivi mobili privati (incluse le app, i programmi, le informazioni personali, ecc.) è in esclusiva responsabilità dei rispettivi proprietari, incluse tutte le componenti hardware interne e/o esterne.
Le sole eccezioni autorizzate con il presente Regolamento consistono nella possibilità, esclusivamente per il personale docente, di utilizzare il dispositivo privato per il mero collegamento alle aree online dei servizi istituzionali, limitatamente a:

- il registro Elettronico scolastico;
- la/e piattaforma/e per la Didattica Digitale Integrata fornita dalla scuola con specifica delibera del Consiglio d'Istituto, adottando preventivamente adeguate misure di sicurezza come ad esempio la preventiva cifratura del documento che contenga informazioni riservate e/o le particolari categorie di dati personali (c.d. sensibili);
- la piattaforma webmail istituzionale (@istruzione.it);

Eventuali ulteriori esigenze riconducibili a situazioni lavorative più ampie, e conseguentemente diversamente implementate, (ad esempio di smart working), andranno definite a parte secondo il dettato della normativa vigente.

Nel caso di utilizzo del dispositivo privato, per le sole eccezioni sopra riportate, gli utenti interessati a tali attività dovranno garantire:

- che il dispositivo non venga mai lasciato incustodito o in disponibilità a terzi privi di titolo;

- che il dispositivo venga protetto con una password o un PIN di accesso (quest'ultimo nel caso dei tablet/smartphone). La password scelta non deve avere relazione con la propria vita privata o istituzionale, deve essere complessa, contenente lettere maiuscole e minuscole, numeri, caratteri speciali, e strutturata fra gli otto ed i quattordici caratteri o il massimo di caratteri consentito dal sistema operativo/software gestionale utilizzato.
- che la password o il PIN di accesso non vengano mai lasciati incustoditi o in disponibilità a terzi privi di titolo, indipendentemente dal tipo di supporto utilizzato;
- che sia abilitato lo screensaver o l'oscuramento dello schermo e che sia previsto il conseguente nuovo accesso mediante inserimento delle proprie credenziali;
- che siano previsti adeguati strumenti di protezione: antivirus e, ove possibile, personal firewall, indipendentemente dal sistema operativo utilizzato dal dispositivo, anche gratuiti;
- che le credenziali concesse dall'Istituto per l'accesso ai servizi istituzionali non vengano, per nessun motivo, memorizzate nel dispositivo, inclusa la compilazione automatica prevista per i browser utilizzati per la navigazione Internet;
- Se il dispositivo personale deve essere utilizzato a scuola (ad esempio per il collegamento alla rete fisica o logica dell'Istituto), l'utilizzo deve essere limitato ai soli scopi istituzionali. In questo caso il proprietario del device si assume qualsiasi responsabilità derivante dall'utilizzo del software presente nel dispositivo, soprattutto se senza licenza d'uso eventualmente presente nel dispositivo privato (D.Lgs. 518/92 sulla tutela giuridica del software e L. 248/2000 sulle nuove norme di tutela del diritto d'autore);
- Se il dispositivo privato consente l'attivazione dei servizi di tethering, ovvero consente la configurazione dell'apparato come gateway per offrire accesso alla Rete Internet per altri dispositivi che ne sono sprovvisti, questo tipo di possibilità va usata solo per periodi molto limitati ed esclusivamente per scopi istituzionali. Il servizio va immediatamente disattivato al termine dell'utilizzo e va protetto da password adeguata.
- L'eventuale periferica WiFi va abilitata sul dispositivo mobile ai fini d'accesso alla rete istituzionale e/o ad altre reti protette e mai pubbliche, e solo ed esclusivamente per il tempo necessario a tali attività.
- Il Bluetooth ed ogni altro protocollo che consenta l'associazione di dispositivi diversi dallo strumento mobile, dev'essere abilitato per l'accoppiamento ai soli strumenti istituzionali in dotazione. Può essere liberamente usato per l'attivazione dell'auricolare personale e/o del kit viva-voce dell'auto. Il Bluetooth non va mai lasciato inutilmente attivo e le password d'associazione non devono mai essere quelle di default previste per il dispositivo.

PRIVATI: SMARTPHONE E TABLET (UTENTI INTERNI E INCARICATI)

Anche per l'uso di smartphone e tablet vale quanto indicato nel capitolo precedente (NOTEBOOK).
In particolare **il ricorso a smartphone/tablet privati per la gestione delle varie attività scolastiche (realizzazione foto e video, utilizzo attivo di programmi di messaggistica istantanea, social, ecc.) può costituire un elevato rischio di sicurezza informatica e di illecito trattamento dei dati personali**.
Non è infatti per nulla scontato che le applicazioni preinstallate dal fornitore del software, e soprattutto quelle successivamente installate dall'utilizzatore, siano in regola con il dettato della normativa vigente. Quasi sempre tali applicazioni richiedono, in varia misura, di poter gestire le telefonate e gli sms, di poter accedere ai contatti ed alla galleria immagini, nonché a molti altri metadati (informazioni che descrivono un insieme di dati, ad es. ID del dispositivo, ID utente, dati pubblicitari, cronologia degli acquisti, posizione particolareggiata o approssimativa, numero di telefono, indirizzo email, interazioni con varie piattaforme, dati di arresto anomalo, dati sulle prestazioni, altri dati diagnostici, informazioni sui pagamenti, altri contenuti dell'utente, ...).
Tutte queste informazioni sono poi trasferite, spesso all'insaputa dell'utente, verso destinazioni assolutamente non sicure dal punto di vista della normativa sulla tutela dei dati personali. Senza considerare che molte delle applicazioni, e spesso gli stessi sistemi operativi, installate o installabili tramite i vari marketplace nascondono anche tracker di profilazione e/o di controllo occulto del dispositivo.
E' evidente quindi come, se non correttamente valutate e gestite, queste applicazioni facciano perdere il controllo sui dati personali e sulle informazioni conservate nel dispositivo, e come quindi possano comportare una specifica responsabilità personale a carico del dipendente/utilizzatore.
Nel caso in cui si renda necessario utilizzare i dispositivi privati (smartphone, tablet o similari) per la realizzazione di fotografie o registrazioni audio/video, tali attività dovranno essere preventivamente autorizzate dalla Direzione, adottando adeguate misure di sicurezza quali la disconnessione dalla rete mobile/dati durante tutte le fasi di realizzazione delle predette attività (acquisizione, conservazione, salvataggio su dispositivi più idonei). In difetto sono da considerarsi vietate.

Furto o smarrimento del dispositivo mobile privato

In caso di furto o smarrimento dei dispositivi mobili privati, il proprietario deve dare tempestiva comunicazione alla Direzione, unitamente ad una dettagliata relazione sottoscritta sul fatto accorso, sul contenuto del dispositivo (qualora fossero conservati dati personali in responsabilità all'Istituto in violazione del presente regolamento), ovvero che i requisiti previsti dal presente regolamento siano stati rispettati, rimanendo a disposizione nel caso sia necessario denunciare l'accaduto all'Autorità Garante e/o ai

diretti interessati oggetto di violazione. Nel caso in cui il dispositivo privato contenga dati personali in responsabilità dell'Istituto, in palese violazione del presente regolamento, le responsabilità civili e penali derivanti saranno ad esclusivo carico del dipendente.

ACCESSO ED USO DEI SISTEMI (UTENTI INTERNI ED ESTERNI, INCARICATI)

PASSWORD

- Tutti gli utenti che si connettono alla rete dell'Istituto tramite autenticazione univoca personale sono tenuti a non rivelare ad alcuno le credenziali di autenticazione (UserID e password), a non memorizzarle nelle impostazioni automatiche dei vari software/gestionali/portali istituzionali, avendo cura di garantire la massima diligenza nella custodia delle stesse e preservandone la segretezza anche durante il momento della digitazione. Qualora l'utente prenda coscienza che qualcuno, chiunque esso sia, possa aver visionato la digitazione o possa essere comunque venuto a conoscenza delle credenziali, deve immediatamente provvedere a cambiarle o a richiederne la sostituzione all'Responsabile IT e alla Direzione.
- Agli utenti è vietato comunicare, scambiare, divulgare o condividere password con altri utenti interni e/o esterni (neppure se appartenenti alla stessa classe, al medesimo gruppo di lavoro o al medesimo ufficio). La condotta non conforme a questa prescrizione può comportare sanzioni disciplinari.
- La password scelta, limitatamente agli utenti interni ed agli incaricati, non deve avere relazione con la propria vita privata o istituzionale, deve essere complessa (lettere maiuscole e minuscole, numeri, caratteri speciali) e di almeno otto caratteri o il massimo di caratteri consentito dal sistema operativo/software gestionale utilizzato.
- E' vietato riutilizzare le proprie password (es. di accesso al pc, alla posta elettronica, alla piattaforma DDI) per la registrazione in altri siti o servizi, anche se utilizzati dall'Istituto.
- Tutti gli utenti devono conservare le password con diligenza per impedire che soggetti terzi ne vengano a conoscenza, segnalando immediatamente al Responsabile IT ed alla Direzione l'eventuale smarrimento, sottrazione o diffusione.
- In nessun caso devono essere annotate password in chiaro, sia su supporto cartaceo sia informatico.

POSTA ELETTRONICA

Il servizio di Posta elettronica è fornito dall'Istituto in funzione della comunicazione, della didattica e delle altre attività strumentali correlate ai fini istituzionali. Il servizio è subordinato all'osservanza integrale delle condizioni contenute nel presente Regolamento. L'utilizzo del servizio da parte dell'Utente costituisce implicita accettazione delle citate condizioni.
E' vietato fornire informazioni riservate o dati personali via mail se non si è certi dell'identità dell'interlocutore; occorre verificare comunque che il soggetto richiedente abbia titolo per poter effettuare la richiesta e che sussistano le disposizioni normative (o l'autorizzazione dell'interessato) che permettano l'eventuale comunicazione dei dati personali.
Ove previsto sono attivati indirizzi di posta elettronica con l'estensione *@nomeistituto.edu.it* (es. *nome.cognome@nomeistituto.edu.it*), con eccezioni previste per i casi di omonimia.
A tale proposito, corre obbligo ricordare che le informazioni istituzionali sono riservate e oggetto di specifica tutela e, come tali, sono sottoposte a misure di sicurezza adeguate a mantenerle segrete da parte dell'Istituto. Pertanto l'uso di caselle di posta private per le comunicazioni istituzionali è tassativamente vietato. Ogni comportamento scorretto potrà anche essere oggetto di specifiche sanzioni disciplinari che potranno variare a seconda della gravità.
La personalizzazione dell'indirizzo non comporta che questo possa essere utilizzato per scopi privati, in quanto trattasi di strumenti di esclusiva proprietà dell'Istituto, messi a disposizione degli utenti al solo fine dello svolgimento del proprio ruolo istituzionale. Non è consentito l'utilizzo per motivi diversi da quelli inerenti all'espletamento degli adempimenti lavorativi o didattici.
Gli utenti saranno responsabili, civilmente e penalmente, dell'attività espletata tramite il proprio account.
Gli utenti non possono utilizzare la posta elettronica istituzionale per inviare, anche tramite collegamenti o allegati in qualsiasi formato, mail che contengano o rimandino a:

- comunicazioni commerciali di qualsiasi tipo;
- proselitismo religioso o propaganda politica;
- materiale in violazione della Legge n. 269 del 1998 (Norme contro lo sfruttamento della prostituzione, della pornografia, del turismo sessuale in danno di minori, quali nuove forme di schiavitù);
- materiale discriminante o lesivo in relazione a razza, sesso, religione, ecc.;
- materiale che violi le normative sulla protezione dei dati personali;
- contenuti o materiali che violino i diritti di proprietà di terzi;
- altri contenuti illegali.

L'elenco riportato è da intendersi meramente esemplificativo e non esaustivo.
In nessun caso l'utente potrà utilizzare la posta elettronica istituzionale per diffondere codici dannosi per i computer quali malware e simili o per perpetrare il furto delle credenziali di altri (pishing).
Gli utenti devono evitare di rispondere alle cosiddette 'catene di Sant'Antonio' che richiedono di inviare un'e-mail a un certo indirizzo o a un certo numero di utenti, poiché possono essere veicoli di diffusione di virus informatici.

E' vietato rispondere a messaggi promozionali o di spamming o pervenuti da mittenti sconosciuti.
Agli utenti è fatto divieto, in via generale, di accedere, in modo non autorizzato, ad altri account, a sistemi o ad altre reti tramite operazioni di pirateria informatica, contraffazione della password o altri mezzi illeciti o fraudolenti, inclusi i casi riconducibili a frode informatica aggravata da furto d'identità digitale (art. 640ter, comma 3, c.p.).
Gli Utenti non potranno utilizzare la posta elettronica istituzionale per trasmettere a soggetti interni e/o esterni all'Istituto le informazioni riservate o documenti Istituzionali, se non nel caso in cui ciò sia necessario in ragione delle mansioni svolte, per l'adempimento di un obbligo di Legge o di contratto di cui sia parte l'Istituto, o al fine di difendere un diritto dello stesso Istituto.
Agli utenti è fatto divieto di utilizzare la funzione 'inoltra' per trasmettere il contenuto delle mail ad altri soggetti diversi dal mittente o dal destinatario, tranne nei casi in cui la comunicazione avvenga utilizzando caselle di posta prive di riferimenti a dati identificativi personali (es.: didattica@nomescuola.edu.it) oppure quando l'inoltro della comunicazione risulti indispensabile per garantire, per motivi organizzativi interni, la trasmissione del contenuto all'ufficio competente.
L'Istituto rende noto agli utenti che, per motivi organizzativi e funzionali, vengono archiviati tutti i messaggi di posta elettronica (anche nelle copie di backup), in uscita ed in entrata dalle caselle di posta elettronica, secondo le modalità previste dalle Leggi vigenti.

ACCESSO ED USO DEI SISTEMI (INCARICATI)

POSTA ELETTRONICA CERTIFICATA (PEC)

La **posta elettronica certificata o PEC** è un tipo particolare di posta elettronica che permette di dare a un messaggio di posta elettronica lo stesso valore legale di una tradizionale raccomandata con avviso di ricevimento, garantendo così la prova dell'invio e della consegna e aggiungendo quindi caratteristiche di sicurezza e di certificazione della trasmissione
Il valore legale è assicurato dai gestori di posta PEC del mittente e del destinatario, che certificano:
- data e ora dell'invio del messaggio dal parte del mittente;
- data e ora dell'avvenuta consegna del messaggio al destinatario;
- integrità del messaggio (e eventuali allegati) nella trasmissione da mittente a destinatario.

I gestori di posta assicurano anche la notifica al mittente e al destinatario di eventuali problemi generatisi durante la trasmissione.
La comunicazione ha valore legale solo se inviata da PEC e ricevuta da PEC.
La casella di Posta Elettronica Certificata dell'Istituto deve accettare esclusivamente documenti provenienti da caselle PEC, contrastando così il fenomeno dello spamming e degli usi impropri.
Il personale preposto all'uso della Posta Elettronica Certificata dovrà utilizzare tale strumento esclusivamente garantendone il valore legale (PEC su PEC), soprattutto nelle trasmissioni che prevedono la comunicazione di particolari categorie di dati personali, che dovranno essere trasmessi solo come allegati, ulteriormente protetti con adeguate misure di sicurezza (ad es. un file protetto da adeguata password di apertura).
Al personale preposto alla protocollazione dei messaggi di posta elettronica certificata è fatto espresso divieto di rendere noto il contenuto delle PEC a chiunque non sia il Dirigente Scolastico, se non previa autorizzazione da parte di quest'ultimo; ogni comportamento scorretto potrà anche essere oggetto di specifiche sanzioni disciplinari che potranno variare a seconda della gravità.
Il personale dipendente preposto all'utilizzo della PEC è tenuto ad accedere alla casella di posta con frequenza almeno giornaliera e a usare tale strumento per tutte le finalità previste per Legge.

MAILING LIST

Allo scopo di facilitare l'interscambio di informazioni istituzionali, è previsto l'uso di "mailing list" limitatamente al solo gruppo interno di indirizzi di posta elettronica autorizzati dall'Istituto con l'estensione *@nomeistituto.edu.it* (es.: personale ATA, Docenti, studenti).
I messaggi generati dovranno obbligatoriamente contenere la lista dei destinatari solo nel campo "*ccn*" (copia carbone nascosta), in modo che ciascun destinatario ne riceva una copia, ma senza poter vedere tutti gli altri destinatari del messaggio stesso. Le eventuali violazioni di tale misura di sicurezza sono da intendersi, a tutti gli effetti, violazione dei dati personali, perseguibili secondo i presupposti di Legge.
Si ricorda che anche per le mailing list valgono le stesse prescrizioni sui contenuti previste per la posta elettronica.

UTILIZZO

È severamente vietato inviare messaggi attraverso lo strumento dell'e-mail che contengano (in allegato o nel corpo del testo) categorie particolari di dati personali (o dati sensibili), senza idonea protezione atta ad impedire la lettura da parte di soggetti non autorizzati (es. un file allegato protetto da adeguata password di apertura).
Nel caso di assenza programmata, al fine di non interrompere, né rallentare i servizi garantiti dall'Amministrazione, l'utente ha la facoltà di predisporre la funzionalità che permette l'invio di un messaggio automatico di risposta che segnali il nominativo di un

collega e il relativo indirizzo di posta, di un collega da contattare nel caso di urgenze. Il soggetto delegato potrà in questo modo ricevere i messaggi di posta elettronica del dipendente assente e a lui indirizzati.
L'utente che si assenterà dovrà altresì prevedere che nel messaggio automatico di risposta siano evidenziati l'inizio e la fine del proprio periodo di assenza.
In alternativa, l'utente potrà nominare una persona di fiducia che, in caso di una sua assenza, potrà avere accesso alla sua casella di posta, al fine di garantire la continuità dell'attività lavorativa. In mancanza di questa nomina e in caso di assenza improvvisa o prolungata, se è necessario e urgente conoscere il contenuto di messaggi di posta elettronica inviati all'indirizzo istituzionale, o per finalità di manutenzione, un soggetto delegato dall'Istituto sarà legittimato a visionare i messaggi di posta elettronica del lavoratore assente, previa comunicazione all'utente (o il suo tentativo).
Il personale dipendente è tenuto ad accedere alla casella e-mail assegnata, con frequenza almeno giornaliera e ad usare tale strumento per qualsiasi comunicazione interpersonale nell'ambito delle finalità lavorative. Le informazioni trasmesse, molto spesso, possono o devono essere condivise, per cui deve essere salvaguardata l'integrità e la confidenzialità dei messaggi e dei contenuti.
È fatto divieto in ogni caso di divulgare a soggetti non autorizzati le notizie, i dati e qualsiasi altra informazione appresa in occasione della ricezione o invio di posta elettronica, in quanto coperte dal dovere di segretezza, a cui sono tenuti i dipendenti pubblici in ottemperanza agli obblighi di Legge.
Al termine della collaborazione lavorativa con l'Istituto per qualsiasi motivo (es. pensionamento, licenziamento, trasferimento presso altro datore di lavoro, ecc.), l'eventuale account nominativo di posta elettronica dell'utente sarà disattivato alla data di cessazione del rapporto di lavoro o di collaborazione. Contestualmente alla disattivazione dell'account si dovrà procedere alla creazione della risposta automatica al mittente di mancato recapito/fallita consegna a cui dovrà seguire la tempestiva cancellazione dell'indirizzo di posta elettronica istituzionale.
Diversamente, nel caso di cui l'indirizzo di posta non sia nominativo, questo non è considerato un dato personale, ma è imputabile esclusivamente all'Amministrazione e pertanto non deve essere obbligatoriamente dismesso.

NAVIGAZIONE IN INTERNET (UTENTI INTERNI ED ESTERNI, INCARICATI)

La finalità dell'accesso e della navigazione in Internet è il reperimento di informazioni e di documenti utili all'Istituto ed ai propri utenti. L'utilizzo per scopi non inerenti ai fini istituzionali non è consentito; ogni comportamento scorretto potrà anche essere oggetto di specifiche sanzioni disciplinari variabili a seconda della gravità.

In considerazione di quanto sopra:
- Durante gli orari in cui vengono svolte le attività istituzionali da parte degli utenti è fatto divieto di navigare in siti non attinenti con le attività didattiche o lavorative, in quanto l'utilizzo del collegamento ad Internet deve essere funzionale alle attività istituzionali.
- Al fine di garantire la sicurezza dei propri dati, nonché per favorire un utilizzo corretto dello strumento Internet, l'Istituto potrebbe adottare alcuni accorgimenti tecnici per prevenire illeciti da parte del personale. E' facoltà dell'Istituto implementare delle misure preventive quali filtri di navigazione avanzati, servizi di Unified Threat Management, proxy server, web filtering (tramite "black list" di siti Internet non consentiti).
- Si sottolinea che in ogni caso la prima e più efficace misura di sicurezza è rappresentata dalla consapevolezza e correttezza dell'utente.
- Non è possibile effettuare il download di file o di software aventi particolari caratteristiche dimensionali, tali da ridurre l'efficienza del sistema (es.: immagini ISO, archivi zip, rar, file eseguibili, mp3, flac, avi, mpeg, divx, mkv, ecc., utilizzo di programmi di file-sharing). Qualsiasi file o programma estraneo a quelli autorizzati e/o che può cagionare incompatibilità con i programmi forniti dall'Istituto, può costituire una minaccia per la sicurezza informatica dell'Istituto. Costituiscono illecito penale anche la illecita duplicazione o riproduzione di software coperto da copyright o non autorizzato. Qualora all'interno dei dispositivi risultino presenti file o software non espressamente autorizzati, potranno essere effettuati dei richiami disciplinari.
- Non è permessa la partecipazione a social network, forum, chat, blog o bacheche elettroniche, mailing list o altri mezzi di comunicazione telematica, anche di messaggistica istantanea, non attinenti con l'attività lavorativa o didattica. Il divieto vale per il pc affidato e comunque a prescindere a nome dell'Istituto, a meno che tali situazioni non siano state preventivamente e formalmente autorizzare dalla Direzione, secondo i requisiti previsti dalla normativa vigente per le pubbliche amministrazioni.

UTILIZZO DEL TELEFONO, FOTOCOPIATRICI E STAMPANTI (INCARICATI)

In via di principio generale, è vietato fornire informazioni riservate o dati personali via telefono se non si è certi dell'identità dell'interlocutore; occorre verificare poi che il soggetto richiedente abbia titolo per poter effettuare la richiesta, nonché che sussistano le disposizioni normative o l'autorizzazione dell'interessato necessari alla comunicazione dei dati personali.
Non deve essere usato il fax per le comunicazioni con altri Enti Pubblici, poiché l'articolo 14 "Misure per favorire la diffusione del domicilio digitale", del c.d. Decreto del Fare (in seguito alle modificazioni apportate dalla legge di conversione n. 98 del 9 agosto

2013) ha stabilito che per la verifica della provenienza delle comunicazioni, è in ogni caso esclusa la trasmissione di documenti a mezzo fax.
Anche l'art. 47 del Codice dell'Amministrazione Digitale ribadisce il divieto di usare il fax nelle trasmissioni di documenti con altre Pubbliche Amministrazioni.
Non esiste nessun obbligo a carico dell'Amministrazione con gli Enti ed i soggetti privati.
I telefoni e le fotocopiatrici devono essere utilizzati per scopi puramente lavorativi.
Non è consentito rivelare numeri telefonici interni o informazioni sull'Istituto a terzi privi di titolo o a soggetti non identificati o identificabili. Ogni comportamento scorretto potrà anche essere oggetto di specifiche sanzioni disciplinari variabili a seconda della gravità.

GESTIONE DELLE COMUNICAZIONI VERBALI

Durante l'attività lavorativa è consuetudine scambiare comunicazioni e informazioni in forma verbale, pertanto si rivela necessario tenere in considerazione i seguenti principi:

- nel corso di conversazioni di lavoro occorre tutelare le informazioni coerentemente con il loro livello di criticità;
- lo scambio di informazioni concernente l'attività lavorativa deve avvenire all'interno di aree che consentano il mantenimento di adeguati livelli di riservatezza;
- tali aree devono rimanere chiuse durante lo svolgimento di riunioni, conversazioni telefoniche, ecc., fra soggetti che siano autorizzati, a pari livello, a trattare le medesime informazioni o gli stessi dati personali;
- nel corso di conversazioni telefoniche, qualora non risulti strettamente necessario, è preferibile non fare ricorso al sistema viva voce. Nel caso debba essere utilizzato tale sistema, l'interlocutore deve essere avvisato prima della sua attivazione;
- prima di condividere verbalmente dati ed informazioni di lavoro occorre accertarsi che la propria controparte, date le mansioni e le responsabilità assegnate, sia autorizzata a venirne a conoscenza;

DOCUMENTAZIONE CARTACEA

La **documentazione cartacea** viene spesso sottovalutata rispetto ai file presenti nel dispositivo informatico messo a disposizione dall'Istituto. La riduzione del numero di fogli stampati rappresenta un grande obiettivo dal punto di vista della salvaguardia delle risorse naturali, ma anche un ottimo sistema per proteggere l'accidentale diffusione di informazioni.
In tale direzione, il Codice dell'Amministrazione Digitale (D.Lgs. 82/2005) prescrive all'art. 40 l'obbligo di creazione e gestione dei documenti originali della Pubblica Amministrazione in modalità informatica.
Si ricordano a titolo esemplificativo alcune misure utili a proteggere la riservatezza e la disponibilità delle informazioni in formato cartaceo:

- porre la massima attenzione per i documenti che si trovano in locali accessibili al pubblico;
- tenere presente che l'accesso agli archivi è consentito al personale espressamente autorizzato in via permanente od occasionale;
- gli archivi storici vanno mantenuti chiusi, compatibilmente con le esigenze di servizio, ed aperti solo quando è necessario;
- bisogna fare ricorso alla stampa solo in caso di reale necessità e comunque il meno possibile;
- in caso di stampa ritirare immediatamente e direttamente i documenti stampati;
- non lasciare mai incustoditi sul proprio tavolo documenti riservati o che contengono particolari categorie di dati personali (c.d. sensibili), anche in caso di assenza breve. In generale riporli sempre in contenitori sottochiave o, ove previsto, distruggerli in modo sicuro quando non più utili;
- la distruzione dei documenti in modo sicuro avviene tramite l'utilizzo di apposita apparecchiatura (c.d. distruggi documenti a frammento secondo la norma DIN 32757 e DIN 66399). Evitare di gettare i documenti interi nel cestino dei rifiuti o del riciclo;
- i documenti devono essere controllati e custoditi dal personale autorizzato in maniera che ad essi non accedano persone prive di autorizzazione, e sono riposti, al termine delle operazioni affidate, negli appositi archivi chiusi a chiave;
- al termine della giornata lavorativa la propria postazione di lavoro deve essere sgombra da tutti i documenti di tipo riservato o che contengono particolari categorie di dati personali (c.d. sensibili) e da quelli ad uso interno, nel caso i cui il posto di lavoro non si trovi in un'area ad accesso riservato od esclusivo.
- le copie dei documenti vanno trattate con la medesima diligenza riservata agli originali;
- la riproduzione di documenti contenenti dati personali è vietata se non espressamente autorizzata.

Si ricorda infine che è fatto espresso divieto di trasferire (es. smart working), anche temporaneamente, in tutto o in parte, gli archivi cartacei storici e/o in corso d'anno al di fuori dei locali preposti nell'Istituto, sia in formato originale che in copia.

PIATTAFORME PER LA DIDATTICA DIGITALE INTEGRATA

Il presupposto per decidere, ove necessario, se, e in che misura, utilizzare a scuola una qualsiasi piattaforma o app di terze parti, soprattutto se prevede il conferimento di dati personali, è quello di dover preventivamente considerare quanto segue:

- I servizi Saas, Paas, Iaas, per poter essere utilizzati nella Pubblica Amministrazione, devono essere obbligatoriamente qualificati dall'Agenzia per la Cyber sicurezza nazionale ai sensi dell'art. 5 par. 1 let. a) del GDPR 2016/679 e secondo il disposto dell'art. 1418 del C.C.;
- Le scuole devono orientarsi verso strumenti che abbiano, fin dalla progettazione ("privacy by design") e per impostazioni predefinite ("privacy by default"), specifiche misure a protezione dei dati (Provvedimento Autorità Garante docweb 9302778/2020). Pertanto le piattaforme vanno valutate preventivamente. E' imperativo quindi limitarsi all'uso di piattaforme che siano state, a vario titolo, autorizzate dalla Direzione dell'Istituto, su cui si possa preventivamente verificare la necessaria adeguatezza con il dettato della normativa vigente;
- Se la piattaforma prescelta comporta il trattamento di dati personali il rapporto con il fornitore dovrà essere regolato con contratto o altro atto giuridico (Provvedimento Autorità Garante docweb 9302778/2020);
- Le scuole dovranno assicurarsi che i dati trattati per loro conto siano utilizzati solo per la didattica a distanza (Regolamento Autorità Garante docweb 9302778/2020).

Un altro aspetto da dover considerare, è che le piattaforme per la didattica digitale integrata devono essere utilizzate, ove questo si renda necessario in base a precise valutazioni in capo al Titolare, solo ed esclusivamente conferendo i dati strettamente necessari alla corretta gestione della didattica (in pratica i soli dati identificativi necessari alla creazione dell'account - nome e cognome – degli utenti/interessati). Ove possibile, e qualora la piattaforma lo permetta, si dovrà obbligatoriamente ricorrere ad account anonimi o pseudonimi (account nei quali gli elementi identificativi sono stati sostituiti da elementi diversi, quali stringhe di caratteri o numeri – hash - oppure sostituendo al nome un nickname, purché sia tale da rendere estremamente difficoltosa l'identificazione dell'interessato). E' vietato perciò conservare in queste piattaforme dati eccedenti e soprattutto qualsiasi tipologia di dati sensibili (sanitari, politici, religiosi o giudiziari), a meno che non vengono messe in atto misure tecniche ed organizzative adeguate di maggior tutela (es. archivi o file preventivamente crittografati prima dell'upload all'interno della piattaforma).
Si ricorda che le uniche piattaforme autorizzate dall'Istituto sono quelle previste nel relativo regolamento (Regolamento DDI esteso), che si richiamano per praticità qui di seguito:
. Registro elettronico NUVOLA madisoft
. Gsuite e Microsoft Teams
Si ricorda altresì che l'eventuale utilizzo di strumenti non ufficialmente riconosciuti dall'Istituto è vietato, a meno che ovviamente non sia fatto a titolo esclusivamente privato; questo però comporta che tali strumenti non potranno e non dovranno essere, per alcun motivo, direttamente e/ indirettamente, riconducibili all'Istituto (es.: utilizzando uno degli account assegnati dall'Istituto, utilizzando il nome e/o il logo della scuola o i riferimenti alla scuola in qualità di docente/studente, ecc.). Trattandosi poi di strumenti utilizzati a scopo esclusivamente privato, corre obbligo evidenziare che la responsabilità nell'utilizzo di tali strumenti sarà ad esclusivo carico dei diretti utilizzatori.

TELEASSISTENZA

Relativamente alle attività di manutenzione remota su personal computer/dispositivo connessi alla rete dell'Istituto, il Responsabile IT ed i tecnici incaricati possono utilizzare specifici software autorizzati esclusivamente dalla Direzione.
Tali programmi sono utilizzati per assistere l'utente durante la normale attività informatica oppure per svolgere l'attività di manutenzione su applicativi. L'attività di assistenza e manutenzione viene concordata preventivamente ed avviene in accordo con l'utente interessato e sotto la sua diretta supervisione. La configurazione del software prevede un indicatore visivo sul monitor dell'utente, che indica quando il tecnico è connesso al dispositivo.

COLLEGAMENTI DA REMOTO

Nel caso in cui sia necessario, limitatamente alla segreteria scolastica, oltre il normale orario d'ufficio, accedere al contenuto dei dispositivi informatici messi a disposizione dall'Istituto, le connessioni dovranno essere gestite esclusivamente a mezzo protocollo VPN (Virtual Private Network). Tali situazioni andranno adeguatamente preventivate ed autorizzate dalla Direzione, previa verifica ed implementazione delle necessarie misure di sicurezza tecniche ed organizzative, da prevedere anche con apposite regolamentazioni ad integrazione del presente regolamento.

FORMAZIONE

La prima misura di sicurezza per la protezione delle informazioni istituzionali e dei dati personali è indubbiamente la preparazione e consapevolezza del personale dipendente nello svolgere il proprio lavoro.

Consapevolezza e preparazione sono aspetti che devono far parte del background del personale dipendente, ma che vanno sviluppati anche attraverso la formazione e l'aggiornamento professionale (corsi di formazione e richiami periodici).
L'Istituto periodicamente procede a interventi formativi specifici per tutti coloro che trattano dati personali e che sono stati istruiti mediante lettera di autorizzazione al trattamento. Questi eventi formativi tratteranno l'analisi dei rischi che incombono sui dati, le misure disponibili per prevenire eventi dannosi, i profili della disciplina sulla protezione dei dati personali, le responsabilità che ne derivano e le misure organizzative e di sicurezza adeguate. La formazione sarà programmata con cadenza annuale.
Il Delegato Privacy istituzionale ed il Responsabile della Protezione dei Dati Personali, sono il punto di contatto per tutto il personale dipendente e gli utenti (interni ed esterni) per le attività che riguardano ed impattano sul trattamento dei dati personali, e rimangono a disposizione per qualsiasi dubbio o segnalazione.
Si ricorda che i corsi di formazione previsti non sono facoltativi e che la mancata ed ingiustificata assenza può portare a provvedimenti di tipo tecnico-disciplinare.

SANZIONI E PROVVEDIMENTI DISCIPLINARI

Il mancato rispetto o la violazione delle regole contenute nel presente Regolamento sono perseguibili con provvedimenti disciplinari anche individuati nel CCNL vigente, nonché, nei casi più gravi, con azioni civili e penali.
Si precisa inoltre che, ai fini dell'efficacia disciplinare, le presenti disposizioni e procedure operative, oltre a essere state pubblicate nelle piattaforme interne, sono disponibili anche nel sito web istituzionale, nella sezione dedicata alle comunicazioni sindacali.

DISPOSIZIONI FINALI (INCARICATI)

SEGRETO D'UFFICIO E INFORMAZIONI RISERVATE

Il personale si impegna, secondo il disposto della normativa vigente (CCNL, art. 326 del C.P., art. 28 della L. 241/90, art. 494 lettera b del D.Lgs. 297/94, D.P.R. n. 62 del 16 Aprile 2013, art. 2 par. 4 del Codice di comportamento dei dipendenti delle pubbliche amministrazioni), a osservare ogni cautela affinché le informazioni in proprio possesso rimangano riservate, essendo inteso che, in caso di comunicazione o divulgazione non autorizzata, sarà a carico dei trasgressori l'onere di provare di avere adottato tali misure di riservatezza.
E' vietato in particolare comunicare e/o divulgare notizie di qualsiasi persona di cui si venga a conoscenza nell'ambito della propria attività lavorativa; soprattutto in considerazione delle attività che prevedono il trattamento di particolari categorie di dati personali.
Il personale non può divulgare, pubblicare o comunicare in alcun modo a terzi privi di titolo (interni ed esterni), direttamente o indirettamente, in tutto o in parte, le informazioni apprese in occasione dello svolgimento delle proprie mansioni, né potrà usarle, sfruttarle o disporne in proprio o tramite terzi, a qualsiasi titolo. Tali comportamenti includono l'inoltro di mail verso l'esterno, se non per attività lavorative, e vietano altresì il re-inoltro ad altri account che non siano quelli istituzionali.
Gli obblighi del dipendente, descritti in questo documento, non termineranno all'atto di cessazione del rapporto di lavoro.

RIEPILOGO MISURE ORGANIZZATIVE E DI SICUREZZA IN AMBITO PRIVACY

- Tutto il personale dipendente che tratta dati è stato autorizzato al trattamento (lettera di nomina o atto di designazione previsti nominalmente nel MOP) ed è tenuto, di conseguenza, al rispetto dei principi e delle misure organizzative e di sicurezza, di cui alla normativa in materia di protezione dei dati personali. In particolare, deve:
  - trattare i dati personali secondo i principi indicati dalla Legge, in modo lecito, corretto e trasparente. Questo significa che deve verificare:
  - verificare se il trattamento sia consentito da una norma di legge o di regolamento;
  - verificare se l'interessato abbia ricevuto idonea informativa e/o abbia eventualmente rilasciato il consenso, ove previsto, ovvero sussista altra base giuridica per il trattamento;
  - controllare la pertinenza e non eccedenza dei dati raccolti e trattati, rispetto alle finalità perseguite, evitando di accogliere dati eccedenti, attuando il principio di minimizzazione nel trattamento;
  - controllare l'esattezza dei dati ed eventualmente, qualora si renda necessario, provvedere al loro aggiornamento;
  - conservare i dati in una forma che consenta l'identificazione dell'interessato per un periodo non superiore a quello necessario agli scopi della raccolta e mettere in atto procedure tali da realizzare la cancellazione degli stessi (ovvero la loro trasformazione in forma anonima) al termine del trattamento, ove previsto;
  - rispettare le procedure di autenticazione informatica e di gestione delle credenziali di autenticazione predisposte dall'Istituto;
  - rispettare le procedure adottate per garantire l'attività di backup e la custodia di copie di sicurezza, salvando i documenti nelle specifiche cartelle di rete a ciò riservate;

- custodire in modo riservato (e per le particolari categorie di dati personali o giudiziari in maniera separata o in archivi chiusi a chiave) le banche dati e comunque ogni documentazione raccolta nello svolgimento dell'attività lavorativa;
- adottare cautele organizzative per garantire che tutte le persone con cui si collabora siano informate sulle regole di riservatezza adottate, e seguire le istruzioni fornite per evitare abusi per negligenza, imprudenza o imperizia;
- verificare sempre l'origine dei dati utilizzati;
- segnalare ai tecnici incaricati, al Responsabile IT o alla Direzione qualsiasi anomalia riscontrata sui sistemi informatici o nella qualità dei dati presenti nel proprio data base;
- attenersi alle istruzioni che sono state e che verranno impartite (mediante apposite lettere di autorizzazione) per garantire la corretta gestione dei dati stessi.

San Martino di Lupari, lì

Istituto Comprensivo di San Martino di Lupari