ITI F. Severi
Via Luigi Pettinati, 46 35129 Padova (PD)
Tel. 049 8658111 - Fax 049 8658120 email: pdtf04000q@istruzione.it

MANUALE PRIVACY
Documentazione redatta in ottemperanza a quanto disposto dal GDPR 2016/679
"*Regolamento generale sulla protezione dei dati*" e dalla normativa nazionale vigente

DISCIPLINARE INTERNO DI SICUREZZA
(Delibera di approvazione C.d.I. n. del)

Indice

0.PREMESSA

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

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;
- L. 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.

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.

La progressiva diffusione delle nuove tecnologie informatiche e l'accesso alla rete Internet espone l'Istituto F. Severi 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 F. Severi 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, ha da tempo deciso di mettere a disposizione dei propri dipendenti adeguate risorse informatiche (computer portatili e/o tablet), 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 agli incaricati 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 l'acquisizione delle competenze digitali. L'accesso alle risorse informatiche dell'Istituto costituisce pertanto un diritto che prevede delle responsabilità in capo all'utilizzatore, o, in caso di studenti minori, a chi esercita la responsabilità genitoriale. 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, limitando le attività esclusivamente a scopi didattici e/o istituzionali. Eventuali violazioni saranno perseguite, ove previsto, in base a quanto disposto nello specifico nei regolamenti sopra indicati, ferme 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. Per tutto quanto non espressamente riportato nel presente Regolamento fanno testo le indicazioni contenute nelle istruzioni relative alle credenziali di accesso alla rete Wi-Fi, alla rete didattica e alla e-mail istituzionale.

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 e le finalità alla base del presente documento, per poter seguire in modo efficace le indicazioni fornite, nel pieno rispetto delle leggi vigenti.

1. NORME COMPORTAMENTALI PER GLI INCARICATI

L'utilizzo degli strumenti informatici dell'Istituto richiede di prendere visione a attenersi a quanto previsto nel presente Regolamento.

- Il personale che tratta dati personali con strumenti informatici è tenuto al rispetto ed 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 spente (salvo indicazioni contrarie da parte del Responsabile IT o della Dirigenza) e libera da documenti che possano implicare il trattamento, da parte di terzi non autorizzati, di informazioni riservate e/o dati personali.
- Se, in orario di servizio, fosse assolutamente necessario lasciare temporaneamente incustoditi i locali e/o gli uffici, il personale dovrà accertarsi di non lasciare attiva la sessione di lavoro nei dispositivi informatici e, se nel locale sono presenti dati personali e/o riservati altrove custoditi (es. armadi) della chiusura di finestre, porte e di tutti gli arredi che li contengono dati.
- 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 su lavagne, 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 e i tablet forniti dall'Istituto, 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, salvo al DSGA e al responsabile dell'Ufficio tecnico e per gli interventi di manutenzione effettuati da personale tecnico o uso didattico.
- 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 o nei dispositivi personali solo per il tempo strettamente necessario al confezionamento di un documento e dovranno essere condivisi solo tramite il registro elettronico.
- Il personale non deve modificare la configurazione del dispositivo che gli viene assegnato. In caso di malfunzionamento, si dovrà richiedere l'intervento dei tecnici preposti, essendo vietata qualsiasi altra iniziativa.
- E' fatto divieto di installare nelle apparecchiature software provenienti da fonti non verificate e comunque non preventivamente autorizzati dalla Dirigenza. Si ricorda in particolare che il mancato rispetto delle norme relative alle licenze d'uso è perseguibile penalmente. L'elenco dei software installati nei dispositivi di uffici e laboratori è predisposto entro il 31 ottobre di ciascun anno scolastico e aggiornato entro il 30 aprile successivo.
- E' assolutamente vietato modificare i dati contenuti nei programmi gestionali salvo gli aggiornamenti necessari in base al profilo professionale, ed è altresì vietato effettuare modifiche, attraverso gli strumenti di sviluppo, di qualsivoglia componente del programma stesso.
- 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.
- È fatto divieto di salvare file e/o cartelle non pertinenti al contesto lavorativo, didattico ed istituzionale o in posizioni non autorizzate, anche in cloud.
- È previsto il salvataggio nel server dell'Istituto di tutti i documenti informatici in capo agli uffici amministrativi contenenti dati personali. 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 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 - es. punti esclamativi sull'icona del programma dell'antivirus, nel menu posto in basso a destra della barra delle applicazioni);

- 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.).

2. NORME COMPORTAMENTALI PER UTENTI INTERNI

L'utilizzo degli strumenti informatici dell'Istituto richiede di prendere visione a attenersi a quanto previsto nel presente Regolamento.

- Lo studente è tenuto al rispetto ed 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 spente al termine della propria sessione di studio, salvo indicazioni contrarie da parte dei docenti.
- I personal computer e i tablet forniti dall'Istituto, utilizzati dagli studenti, sono strumenti didattici. Ogni utilizzo improprio può causare disservizi, ulteriori costi di manutenzione e soprattutto minacce alla sicurezza e alla protezione dei dati personali in essi contenuti. 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 dal Docente. La responsabilità dei contenuti nei dispositivi di memoria, ove consentiti, resta a totale carico dei rispettivi proprietari o, nel caso di studenti minori, di chi esercita la responsabilità genitoriale su di essi.
- Lo studente non deve modificare la configurazione del personal computer a cui viene assegnato; in caso di malfunzionamento dovrà segnalare l'accaduto ai docenti, che avranno cura di richiedere l'intervento dei soli tecnici preposti. 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.
- 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.
- 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.).

3. NORME COMPORTAMENTALI PER UTENTI ESTERNI

Anche per gli utenti esterni (fornitori, formatori, stagisti, collaboratori della scuola per attività formative o di segreteria) valgono le stesse indicazioni previste per gli studenti, fermo restando che, nel caso di utilizzo degli strumenti informatici dell'Istituto, dovrà essere prevista obbligatoriamente la creazione di account specifici.

4. GESTIONE SISTEMI INFORMATIVI

4.1 PASSWORD

L'accesso ad ogni postazione di lavoro individuale, alla rete e alle applicazioni in uso avviene mediante password personali. Le password sono utilizzate per accedere a differenti profili di autorizzazione nell'ambito del sistema informativo (es. utenze contabilità, accesso ad Internet, sistemi di posta elettronica, ecc.). Si raccomanda di evitare password di facile individuazione, come a esempio quelle che

- 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.).

Sono da ritenere password di soddisfacente sicurezza quelle composte da caratteri maiuscoli, minuscoli, numeri e caratteri di interpunzione, come [ ] ! ? * " , ;

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 online (in 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.

4.2 SALVASCHERMO

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 Dirigenza.

4.3 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 contengano dati personali, devono essere salvati sempre anche nel disco di rete e, una volta che non sussistano più ragioni di convenienza, i suddetti file locali devono essere eliminati a favore della sola conservazione sul disco di rete. Le cartelle nei dischi di rete possono essere create per uffici/classi, per competenza o per singolo utente (vedere anche il punto successivo per la cartella personale nei dischi di rete).
Le password di accesso alla rete, ai relativi dischi ed ai programmi sono personali e vanno gestite secondo le procedure previste. È assolutamente proibito autenticarsi nella rete e nei programmi con nomi utente diversi da quelli consegnati all'inizio.

4.4 CARTELLE PERSONALI

Nei dischi di rete sono presenti cartelle nominative per il salvataggio dei propri dati. In tali cartelle devono essere salvati tutti i file di cui l'Istituto ha obbligo di conservazione, anche se memorizzati temporaneamente in locale su personal computer.
In caso di furto o smarrimento dei dispositivi, 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.

4.5 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 se le informazioni non sono adeguatamente e preventivamente protette (es.: cifratura tramite protezione con password adeguata) e se tali attività non sono autorizzate dalla Dirigenza.
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 il 'Responsabile IT o i tecnici incaricati.

5. 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.

5.1 LABORATORI MOBILI

I laboratori mobili sono armadi di PC o di tablet, questi ultimi in fase di predisposizione, dotati di ruote e prenotabili dai docenti che intendono utilizzarli durante le lezioni in classe. Sono da considerarsi alla stregua dei laboratori allestiti negli appositi locali della scuola. Valgono pertanto i regolamenti, divieti e tutto ciò che è espresso nel presente disciplinare. Nel caso specifico di laboratori mobili costituiti da tablet, risulta necessario adottare un registro cartaceo (in dotazione a ciascun carrello), dove il docente che ha prenotato il carrello dovrà annotare il nominativo dell'utilizzatore e l'ora sia di consegna che di restituzione del dispositivo.

5.2 DI PROPRIETÀ DELL'ISTITUTO CONCESSI IN USO AGLI INCARICATI, IN COMODATO D'USO A UTENTI INTERNI O A UTENTI ESTERNI PER USO TEMPORANEO

I dispositivi mobili sono assegnati individualmente ai richiedenti in casi specifici, previa sottoscrizione di contratto di comodato d'uso; i comodatari rispondono del loro utilizzo e devono custodirli con diligenza, sia durante gli spostamenti, sia durante l'eventuale utilizzo intra ed extra Istituto.
Dispositivi mobili possono essere concessi a utenti esterni (es., formatori, esperti esterni), limitatamente al tempo in cui si trattengono nei locali della scuola per svolgere l'attività.
Ai dispositivi mobili concessi in comodato 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.
E' vietato l'uso di qualsiasi dispositivo esterno collegabile al dispositivo mobile, se non quelli istituzionali o autorizzati.
L'utilizzatore che abbia necessità di apportare modifiche hardware o software al dispositivo mobile in dotazione deve farne preventiva richiesta alla Dirigenza o al Responsabile IT.
Al momento della riconsegna, 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 saranno rimossi.

<u>Disposizioni operative per l'utilizzo dei dispositivi mobili.</u>

- 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.
- E' fatto espresso divieto di memorizzare nel dispositivo mobile qualsiasi credenziale che permetta l'accesso ad aree riservate in responsabilità all'Istituto.
- Nel caso di dispositivi di proprietà dell'Istituto è vietato utilizzare qualsiasi software e/o tecnica di jailbreak (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, provenienti da fonti non verificate e senza autorizzazione da parte del Responsabile IT, della Dirigenza o - solo nel caso degli studenti con tablet - del docente coordinatore della classe. 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).
- In caso di furto o smarrimento, l'utente dovrà informare tempestivamente la Dirigenza e produrre denuncia presso le autorità competenti.
- 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 informare tempestivamente il Responsabile IT o la Dirigenza.
- Non è consentito all'utilizzatore disattivare l'antivirus, in tutto o in parte.
- È vietato l'utilizzo dei servizi di tethering.
- È vietato abilitare il WiFi su reti pubbliche.

5.3 DI PROPRIETÀ PERSONALE: NOTEBOOK

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.
L'uso del dispositivo in orario di servizio è vietato al personale, tranne nei seguenti casi: accesso a

- registro elettronico;
- 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);
- software per l'attività didattica;
- piattaforma webmail istituzionale (@itiseveripadova.edu.it o @istruzione.it) per comunicazioni di servizio indifferibili.

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 comunque 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). Per la scelta della password si rinvia al paragrafo "Gestione della password";
- che la password o il PIN di accesso non vengano mai lasciati incustoditi o in disponibilità a terzi privi di titolo;
- 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;
- il proprietario del device si assume qualsiasi responsabilità derivante dall'utilizzo del software presente nel dispositivo, soprattutto se 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);
- il servizio di tethering è autorizzato esclusivamente
    - ai docenti in caso di necessità di malfunzionamento della rete di Istituto, per lo stretto periodo di tempo necessario,
    - agli utenti esterni per lo svolgimento dell'attività prevista;
- l'accesso alla rete WiFi di Istituto va abilitato solo ed esclusivamente per il tempo necessario a svolgere l'attività.

Gli studenti possono utilizzare i loro dispositivi personali (compreso l'eventuale servizio di tethering) solo previa espressa autorizzazione del docente e per finalità didattiche.

5.4 DI PROPRIETÀ PERSONALE: SMARTPHONE E TABLET

Per l'uso di smartphone e tablet valgono le regole indicate nel capitolo precedente (NOTEBOOK). Inoltre, 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 Dirigenza e adottate 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.

Si evidenzia infatti che il ricorso a smartphone/tablet privati per la gestione delle varie attività scolastiche (realizzazione di 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 scontato che le applicazioni preinstallate dal fornitore del software, e soprattutto quelle successivamente installate dall'utilizzatore, siano in regola con quanto prevede la legge. Quasi sempre tali applicazioni richiedono, in varia misura, di poter gestire telefonate e sms, di poter accedere ai contatti e 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, ...).
Queste informazioni sono poi trasferite, spesso all'insaputa dell'utente, verso destinazioni non sicure dal punto di vista della tutela dei dati personali. Inoltre, molte delle applicazioni installate o installabili tramite i marketplace (spesso gli stessi sistemi operativi) nascondono tracker di profilazione e/o di controllo occulto del dispositivo. Se non correttamente valutate e gestite, queste applicazioni fanno perdere il controllo sui dati personali e le informazioni conservate nel dispositivo e possono comportare una specifica responsabilità personale a carico del dipendente/utilizzatore.

Furto o smarrimento del dispositivo mobile privato

In caso di furto o smarrimento dei dispositivi mobili privati, il proprietario deve dare tempestiva comunicazione alla Dirigenza, 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.

6. ACCESSO E USO DEI SISTEMI

6.1 RETE (PER TUTTI)

- 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 oppure certificato digitale), 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 Dirigenza.
- 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 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.
- 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.

6.2 POSTA ELETTRONICA (PER TUTTI)

Il servizio di posta elettronica è fornito dall'Istituto solo in funzione delle altre attività strumentali 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. Al termine del rapporto con l'Istituto per qualsiasi motivo, l'account nominativo di posta elettronica sarà disattivato entro 30 giorni.

E' vietato fornire informazioni riservate o dati personali via mail senza adottare preventivamente, prima di inviare la mail, adeguate misure di sicurezza (es.: documento allegato con accesso ai contenuti tramite software o impostazioni di sicurezza avanzate).
Gli indirizzi di posta elettronica hanno generalmente la forma
per il personale: *nome.cognome@itiseveripadova.edu.it*, con eccezioni in casi di omonimia;
per gli studenti: cognomematricola@itiseveripadova.edu.it;
e di funzioni o servizi generali
(es. dirigente@itiseveripadova.edu.it, orientamento@itiseveripadova.edu.it).

Le informazioni istituzionali riservate sono oggetto di specifica tutela e, come tali, sottoposte a misure di sicurezza adeguate a mantenerle segrete da parte dell'Istituto. In questi casi, l'uso di caselle di posta

private 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 autorizza l'uso per scopi privati, in quanto strumento di esclusiva proprietà dell'Istituto, messo a disposizione degli utenti al solo fine dello svolgimento del proprio ruolo istituzionale. Non è consentito l'utilizzo per motivi diversi da quelli inerenti l'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 (phishing).
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, 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 e in ogni caso vanno assunte tutte le opportune misure di protezione (es. allegati protetti da password).
Agli utenti è fatto divieto di utilizzare la funzione 'inoltra' per trasmettere il contenuto delle mail a 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.: pdtf04000q@istruzione.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 tutti i messaggi di posta elettronica, in uscita ed in entrata dalle caselle di posta elettronica, vengono archiviati secondo le modalità e procedure stabilite da Google LLC per la piattaforma Google Workspace for Education.

6.3 POSTA ELETTRONICA CERTIFICATA (PEC) (PER INCARICATI)

La posta elettronica certificata o PEC è la versione telematica della posta raccomandata con avviso di ricevimento, con prova dell'invio (data, ora) e della consegna (data, ora) nella casella di posta PEC del destinatario, con garanzia di integrità del messaggio (e eventuali allegati). Eventuali problemi generatisi durante la trasmissione sono notificati al mittente.
Dati personali trasmessi a mezzo PEC vanno preventivamente protetti e i contenuti mantenuti riservati.
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 dipendente preposto all'utilizzo della PEC è tenuto ad accedere alla casella di posta con frequenza almeno giornaliera.

6.4 GRUPPI (PER INCARICATI E UTENTI INTERNI)

I docenti possono utilizzare la funzionalità "Gruppi Classe" per trasmissioni di materiali e comunicazioni con gli studenti, con l'avvertenza di evitare in ogni modo la trasmissione/ricezione di contenuti di carattere personale/riservato/sensibile.
Gli studenti non devono utilizzare la funzionalità "Gruppi Classe" se non con espressa autorizzazione del docente.

6.5 MAILING LIST (PER TUTTI)

Eventuali mailing list possono essere utilizzate solo con le stesse prescrizioni sui contenuti previste per la posta elettronica e 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.

6.6 NAVIGAZIONE IN INTERNET (PER TUTTI)

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.
- Fatto salvo che la prima e più efficace misura di sicurezza è rappresentata dalla consapevolezza e correttezza dell'utente, 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).
- 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 assunte misure 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 anche per i dispositivi personali quando collegati alla rete dell'Istituto, a meno che tali situazioni non siano state preventivamente e formalmente autorizzate dal Dirigente Scolastico, secondo i requisiti previsti dalla normativa vigente per le pubbliche amministrazioni.

6.7 UTILIZZO DEL TELEFONO, FOTOCOPIATRICI E STAMPANTI (PER INCARICATI)

È vietato fornire al telefono informazioni riservate e dati personali. I telefoni, le fotocopiatrici e le stampanti devono essere utilizzati solo per stretta e dimostrabile necessità e per scopi puramente lavorativi.
Ogni comportamento scorretto potrà essere oggetto di provvedimento disciplinare variabili a seconda.

6.8 GESTIONE DELLE COMUNICAZIONI VERBALI (PER INCARICATI)

Durante l'attività lavorativa è consuetudine scambiare comunicazioni e informazioni in forma verbale, pertanto è 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., e sono consentite solo tra soggetti 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.

6.9 DOCUMENTAZIONE CARTACEA (PER INCARICATI)

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.
Nel caso sia necessario produrre documenti cartacei, si forniscono, a titolo esemplificativo, alcune misure utili a proteggere la riservatezza e la disponibilità delle informazioni:

- evitare la collocazione in locali accessibili al pubblico;
- tenere presente che l'accesso agli archivi è consentito solo al personale espressamente autorizzato, in via permanente o 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;
- 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 sotto chiave 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 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 in 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.

6.10 PIATTAFORME PER LA DIDATTICA DIGITALE INTEGRATA (PER INCARICATI)

Le piattaforme utilizzate dall'Istituto per la didattica digitale integrata sono Google Workspace for Education e il Registro Elettronico di Spaggiari (applicazioni Classeviva e Scuola&Territorio).
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 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 limitarsi all'uso di piattaforme che siano state, a vario titolo, autorizzate dalla Dirigenza 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 (Regolamento Autorità Garante docweb 9302778/2020).

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 (la tipologia di dati trattata dipende sia dalla piattaforma che dalla tipologia di utente e trova la sua disciplina nei rispettivi regolamenti).
E' vietato 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 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.

7. CONTROLLI

Ferme restando le misure di sicurezza perimetrali attivate dall'Istituto (antivirus, firewall, blacklist siti web, ecc.), la scuola si riserva la facoltà, nel rispetto della tutela del diritto alla riservatezza e del principio di proporzionalità e non eccedenza, di svolgere dei controlli indiretti, mirati e non sistematici, che consentano di verificare l'effettiva conformità dell'uso degli strumenti informatici alle presenti prescrizioni, mediante l'ausilio dell'amministratore di sistema o (se necessario) di personale esterno appositamente autorizzato.
Al fine di verificare la funzionalità, la sicurezza del sistema ed il suo corretto utilizzo, le apparecchiature di rete memorizzano in specifici file di log, le informazioni relative ai siti che i dispositivi informatici hanno visitato. L'accesso a questi dati è effettuato dal Responsabile IT. L'Istituto, secondo le previsioni di cui al Regolamento del Garante in materia di trattamento dati personali (Regolamento del 1° marzo 2007), effettua il monitoraggio generalizzato ed anonimo dei log di connessione. Nel rispetto al principio di finalità, pertinenza e non eccedenza, tali log sono conservati negli archivi dell'Istituto per 30 giorni. L'eventuale prolungamento dei termini di conservazione è da considerarsi eccezionale e può avere luogo solo in relazione all'esercizio o alla difesa di un diritto in sede giudiziaria, oppure per l'obbligo di custodia dei dati al fine di ottemperare ad una specifica richiesta dell'Autorità Giudiziaria.
In ogni caso, solo il Dirigente Scolastico, supportato da Responsabile IT, potrà accedere a tali informazioni.
Inoltre la Dirigenza, tramite il Responsabile IT, nel caso sia necessario procedere a un controllo per garantire la piena sicurezza della rete o per motivi di manutenzione, si riserva di analizzare i dispositivi informatici ad uso promiscuo, quali le digital board, gli account e-mail istituzionali non nominali (es.: pdtf04000q@istruzione.it), le cartelle condivise presenti nelle varie reti istituzionali (es.: server, unità di backup, aree cloud).
Nel caso di dispositivi informatici ad uso esclusivo di un dipendente/utente o di dispositivi accessibili con credenziali esclusive, quali i computer, le caselle di posta nominali, le aree riservate contenute nelle cartelle condivise nelle varie reti istituzionali (es.: server, unità di backup, aree cloud), i controlli potranno svolgersi, senza analizzare il contenuto del materiale presente, attraverso le seguenti fasi:

- analisi aggregata (cioè che non permette l'identificazione univoca del/i soggetto/i) del traffico di rete riferito all'intera struttura lavorativa od a sue specifiche aree (e-mail, file, accesso a contenuti e servizi) anche tramite attivazione di specifici alert sui flussi dei dati;
- analisi aggregata di eventuali ambienti di sviluppo (c.d. sandbox) riferiti all'intera struttura lavorativa od a sue specifiche aree (e-mail, file, accesso a contenuti e servizi) anche tramite attivazione di specifici alert sui flussi dei dati;
- analisi aggregata sull'occupazione dello spazio di memorizzazione sui server/aree cloud istituzionali.

I controlli, proporzionati e non eccedenti anche rispetto allo scopo di verifica dell'adempimento contrattuale, non potranno mai svolgersi direttamente e in modo puntuale, ma saranno preliminarmente compiuti su dati aggregati, riferiti all'intera struttura dell'Istituto.
A seguito di detto controllo anonimo, potrà essere emesso un avviso generalizzato di rilevazione di eventuali anomalie nell'utilizzo dei presidi tecnologici, con l'invito ad attenersi scrupolosamente a compiti assegnati e alle istruzioni impartite.
Non saranno comunque ammessi controlli prolungati, costanti o indiscriminati.

In considerazione degli obblighi di vigilanza sugli studenti, che devono anche garantire lo sviluppo, la responsabilizzazione e la crescita personale degli stessi, i controlli che la scuola potrà effettuare sulle attività che comportino il ricorso all'infrastruttura informatica dell'Istituto sono i seguenti:

- controlli diretti e tempestivi sulla navigazione Internet degli studenti con conservazione dei log fino ad un massimo di 30 giorni;
- controlli nei dispositivi (es: personal computer, notebook, ecc.) in uso agli studenti, anche se in rete di dominio (active directory) con accesso nominativo. L'uso di credenziali nominative in questo caso si deve intendere non per garantire la confidenzialità dei dati, ma l'identificabilità della responsabilità dell'utente;
- controlli nei dischi di rete condivisi, nelle aree (es.: Drive) interne alle piattaforme DDI condivise, ecc…

La Dirigenza, in evidenza di acclarate attività non conformi, provvederà ad informare, nei casi previsti, le autorità competenti.

8. TELEASSISTENZA (PER INCARICATI)

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.

9. COLLEGAMENTI DA REMOTO (PER INCARICATI)

Nel caso in cui sia necessario, limitatamente alla segreteria scolastica, accedere al contenuto delle risorse informatiche messe 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 Dirigenza, previa verifica ed implementazione delle necessarie misure di sicurezza tecniche ed organizzative. Accessi e durata del collegamento sono registrati.

10. FORMAZIONE (PER INCARICATI)

La prima misura di sicurezza per la protezione delle informazioni istituzionali e dei dati personali è la preparazione e consapevolezza del personale dipendente nello svolgere il proprio lavoro, da sviluppare 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 ricevono lettera di autorizzazione al trattamento.
Gli eventi formativi devono trattare 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 è programmata con cadenza annuale.
Il Delegato Privacy istituzionale ed il Responsabile della Protezione dei Dati Personali sono il contatto per tutto il personale dipendente e gli utenti (interni ed esterni) per le attività che riguardano e impattano sul trattamento dei dati personali, e sono a disposizione per qualsiasi dubbio o segnalazione.
La formazione è obbligatoria.

11. SANZIONI E PROVVEDIMENTI DISCIPLINARI

Il mancato rispetto o la violazione delle regole contenute nel presente Regolamento sono perseguibili con provvedimenti disciplinari e nei casi più gravi, con azioni civili e penali.
Si precisa che, ai fini dell'efficacia disciplinare, le presenti disposizioni e procedure operative, oltre a essere state pubblicate sul registro elettronico, sono consultabili sul sito web istituzionale nella sezione "Regolamenti".

12. DISPOSIZIONI FINALI (PER INCARICATI)

12.1 SEGRETO D'UFFICIO E INFORMAZIONI RISERVATE

Il personale è tenuto, 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 dati personali 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; è in ogni caso vietato il re-inoltro ad altri account che non siano istituzionali.
Gli obblighi del dipendente descritti in questo documento sono perenni (non terminano all'atto di cessazione del rapporto di lavoro).

12.2 RIEPILOGO MISURE ORGANIZZATIVE E DI SICUREZZA IN AMBITO PRIVACY

Tutto il personale dipendente che tratta dati deve essere autorizzato al trattamento (lettera di nomina o atto di designazione previsti nominalmente nel MO); in conseguenza dell'incarico è tenuto 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 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;
- verificare la pertinenza e non eccedenza dei dati raccolti e trattati, rispetto alle finalità perseguite, evitando di accogliere dati eccedenti (principio di minimizzazione nel trattamento);
- verificare l'esattezza dei dati e, 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 (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 Dirigenza qualsiasi anomalia o errore riscontrato sui sistemi informatici;
- attenersi alle istruzioni che sono state e che verranno impartite (mediante apposite lettere di autorizzazione) per garantire la corretta gestione dei dati stessi.

13. ENTRATA IN VIGORE DEL REGOLAMENTO

Il presente regolamento entra in vigore il giorno successivo alla delibera di approvazione da parte del Consiglio di Istituto; contestualmente, tutte le disposizioni in precedenza adottate in materia, in qualsiasi forma comunicate, devono intendersi abrogate e sostituite dalla presente.

Padova, ….....

Istituto I.T.I. F. Severi