Ministero dell'Istruzione e del Merito
Istituto Comprensivo "E. Fermi", via Cavour,9 - 24030 Carvico
Tel. 035 4380362 – 035 4398788 Fax 035 4380379
email uffici bgic8360g@istruzione.it email pec bgic83600g@pec.istruzione.it
sito web : www.iccarvico.edu.it - codice fiscale 91025980169
codice IPA: istsc_bgic83600g - codice univoco per la fatturazione: UF8CAU

Disciplinare per l'uso delle risorse informatiche locali (inclusi i servizi di rete) dell'Istituto Comprensivo Statale "E.Fermi" di Carvico

Data ultima revisione: 18 febbraio 2023

Approvato con Delibera del Consiglio d'istituto n.109
del 27 febbraio 2023

Sommario

Finalità

L'Istituto Comprensivo Statale "E.Fermi" di Carvico (nel seguito, Istituto) è un'istituzione scolastica autonoma del sistema educativo di istruzione e formazione nazionale. L'Istituto considera le risorse informatiche ed i servizi di rete, nonché i dati e le informazioni da questi trattati, funzionali al raggiungimento delle proprie finalità istituzionali di insegnamento, educazione, formazione e ricerca in ambito pedagogico e didattico.

Con il presente Disciplinare l'Istituto intende:

- salvaguardare la sicurezza del proprio sistema informatico, inteso come il complesso unitario delle risorse informatiche dei sei plessi dell'Istituto (scuola primaria e scuola secondaria di primo grado di Carvico, scuola primaria e scuola secondaria di primo grado di Sotto il Monte G.XXIII, scuola primaria e scuola secondaria di primo grado di Villa d'Adda);
- assicurare la funzionalità delle strumentazioni informatiche in dotazione all'Istituto;
- tutelare la riservatezza, l'integrità e la disponibilità dei sistemi informatici e delle informazioni e dei dati, anche personali, da questo prodotti, raccolti o comunque trattati;
- prevenire l'utilizzo indebito dei sistemi informatici e dei dati raccolti attraverso tali sistemi;
- adottare limiti e cautele per evitare la registrazione e diffusione di fotografie, audio e filmati in tempo reale anche utilizzando dispositivi di telefonia mobile;
- indicare in modo particolareggiato quali siano gli strumenti messi a disposizione, le modalità di utilizzo nell'organizzazione dell'attività lavorativa e/o di studio degli strumenti informatici messi a disposizione del personale e degli studenti;
- precisare in che misura e con quali modalità vengono effettuati i controlli;
- tutelare sia i lavoratori interessati nel trattamento di dati per finalità di gestione del rapporto in ambito pubblico sia gli studenti e i loro genitori, adottando quelle misure che garantiscono un elevato standard di sicurezza e garanzia;
- garantire che il trattamento dei dati raccolti in relazione all'uso delle risorse informatiche e dei servizi di rete avvenga solo per finalità determinate, esplicite e legittime, nel rispetto dei principi di necessità, pertinenza, correttezza e non eccedenza secondo quanto previsto dal Regolamento UE 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali (noto come *General Data Protection Regulation*, ossia GDPR dal suo acronimo). Nel seguito di questo documento ci si riferirà a tale atto con il termine Regolamento.
- garantire che i sistemi informativi e gli applicativi informatici siano pertanto configurati in modo da ridurre al minimo l'utilizzo dei dati personali e identificativi.

Campo di applicazione e definizioni

Le presenti istruzioni operative disciplinano l'utilizzo delle risorse informatiche locali nei plessi dell'Istituto Comprensivo Statale "E.Fermi" di Carvico (nel seguito, Istituto) e si applicano **alle risorse informatiche** (inclusi i **servizi di rete**), così definite:

- **qualunque dispositivo** (PC, notebook, Chromebook, Digital Board, LIM, tablet, stampanti, scanner o altre periferiche, sistemi di storage, dispositivi di realtà aumentata e virtuale, … - nel seguito, dispositivi locali), di proprietà dell'Istituto o **comunque disponibile nei plessi dell'Istituto o connesso alla rete dell'Istituto**;

- **apparati e infrastrutture di rete** di proprietà dell'Istituto o dei Comuni proprietari degli immobili o comunque connessi alla rete dell'Istituto;
- il **servizio di connettività alle reti locali e geografiche** con esclusione della mera connettività geografica garantita tramite accordi con i Comuni proprietari ovvero il Ministero delle imprese e del made in Italy nell'ambito del Piano strategico Banda ultralarga;
- **istanze virtuali** di calcolatori o apparati di rete;
- **software e dati** acquistati, prodotti o pubblicati dall'Istituto, dai docenti, dagli studenti e in generale dal personale dell'Istituto.

Le finalità d'uso delle risorse informatiche rete riguardano l'impiego in ambito informativo, documentario, di ricerca e di didattica, di aggiornamento e attività collaborative fra scuole ed enti, di adempimento degli obblighi di legge.

Non è ammesso l'utilizzo delle risorse informatiche e dei servizi di rete per scopi personali.

Tutti coloro ai quali è consentito l'accesso alle risorse informatiche e ai servizi di rete sono tenuti al rispetto delle norme di seguito esposte, che definiscono ed integrano i doveri minimi di condotta previsti nel Codice di Comportamento dei dipendenti dell'Istruzione e del Merito, dello Statuto delle Studentesse e degli Studenti, oltre comunque a un comportamento ispirato ai principi di correttezza e diligenza.

Le regole del presente disciplinare si applicano anche al personale delle ditte che effettuano attività di manutenzione dei sistemi informativi e delle reti, nonché agli eventuali altri soggetti autorizzati all'accesso sulla base di convenzioni o accordi.

L'utilizzo dei sistemi informatici di segreteria e delle attrezzature delle aule informatiche e speciali sono regolate, ad integrazione e non in sostituzione delle norme dettate nel presente disciplinare, dal Regolamento per l'uso delle aule informatiche e delle aule speciali che sarà rivisto in funzione dell'introduzione delle tecnologie di realtà aumentata e virtuale e dell'intelligenza artificiale.

I soggetti che operano con le risorse informatiche dell'istituto si distinguono in:

• **Utente**: ogni soggetto che abbia accesso alle risorse informatiche dell'Istituto, in relazione alle funzioni ed attività che svolge nell'ambito dell'Istituto;
- **Referenti delle aule informatiche dei plessi**: sono i docenti individuati dal Dirigente con compiti di monitoraggio, supporto immediato ai docenti dei plessi, supervisione delle attrezzature delle aule informatiche e delle reti dei plessi. Controllano in particolare che sui dispositivi locali siano rispettate le regole in materia di cifratura dei dati e di utilizzo dei file vault. Segnalano al Servizio informatico d'istituto eventuali dispositivi non protetti da antivirus o non aggiornati. Collaborano su richiesta alle operazioni di censimento dei dispositivi attivi. Essi coordinano gli utenti e l'uso delle risorse locali di ciascun plesso, in conformità alle indicazioni del presente disciplinare e dell'Amministratore di sistema;

• **Amministratore di sistema**: figura professionale dedicata alla gestione e alla manutenzione di impianti di elaborazione con cui vengano effettuati trattamenti di dati, anche personali, compresi i sistemi di gestione delle basi di dati, le reti locali e gli apparati di sicurezza, individuato d'intesa con i Comuni proprietari degli edifici scolastici;

• **Servizio informatico d'Istituto**: è il servizio cui compete la gestione delle risorse informatiche dell'Istituto, i collegamenti in rete all'interno ed all'esterno di ciascun plesso, nonché la cura,

installazione e sviluppo delle stesse e l'assistenza agli utenti per l'accesso alle risorse ed alla rete; ha inoltre competenza in materia di sicurezza su ogni risorsa informatica comunque afferente alla scuola. È composto dall'animatore digitale, dall'assistente tecnico, dall'amministratore di sistema e da un referente per la segreteria.

- **Dirigente:** il soggetto che assume la qualifica di dirigente scolastico *pro tempore* dell'Istituto.

Accesso alle risorse informatiche

L'accesso alle risorse informatiche e ai servizi di rete dell'Istituto è consentito, previa identificazione, ai dipendenti e agli studenti. Possono essere autorizzati all'accesso anche collaboratori o altri autorizzati secondo le norme del presente Disciplinare.

L'autorizzazione all'accesso è rilasciata dal Dirigente o da un suo delegato per un periodo temporale limitato alla durata del rapporto sulla base del quale è consentita l'attività all'interno dell'Istituto.

L'accesso è personale, non può essere condiviso o ceduto e il relativo utilizzo è consentito a ciascun utente soltanto in conformità alle norme del presente Disciplinare.

Disposizioni generali per l'uso delle risorse informatiche

Le risorse informatiche, in quanto essenziali per l'istituto, sono rese disponibili esclusivamente per il conseguimento delle finalità istituzionali dell'Istituto stesso.

Gli utenti sono tenuti a servirsi delle risorse informatiche dell'Istituto prestando il proprio contributo affinché ne sia preservata l'integrità e garantito il buon funzionamento.

Sono pertanto vietate:

1. attività contrarie alla legge nazionale, alle disposizioni dell'Unione europea e del diritto internazionale o proibite dai regolamenti e dalle consuetudini d'uso delle reti e dei servizi acceduti;
2. attività commerciali, o comunque lucrative, non autorizzate, nonché la trasmissione di materiale commerciale e/o pubblicitario non richiesto (spamming) o l'uso delle proprie risorse da parte di terzi per tali attività;
3. attività comunque idonee a danneggiare, distruggere, compromettere la sicurezza delle risorse informatiche dell'Istituto o dirette a violare la riservatezza e/o cagionare danno a terzi, ivi inclusa la creazione, trasmissione e conservazione di immagini, dati o altro materiale offensivo, diffamatorio, osceno, indecente o che attenti alla dignità umana, specialmente se riguardante il sesso, la razza, la religione, le opinioni politiche o la condizione personale o sociale;
4. attività che pongano in essere un trattamento illecito di dati personali;
5. attività comunque non conformi ai fini istituzionali dell'Istituto.

Disposizioni specifiche per l'uso delle risorse informatiche

Al fine di garantire la sicurezza delle risorse informatiche e dei servizi di rete è vietato:
1. connettere risorse informatiche alla rete locale o ad altri servizi che includono la connettività di rete senza l'autorizzazione del Servizio informatico d'Istituto;
2. cablare, collegare o modificare apparati di rete senza l'autorizzazione del Servizio informatico d'Istituto;

3. utilizzare indirizzi di rete e nomi non espressamente assegnati;
4. installare sistemi, hardware o software, che consentano accesso alle risorse informatiche senza l'autorizzazione del Servizio informatico d'Istituto;
5. fornire accesso alle risorse informatiche a soggetti non espressamente autorizzati;
6. divulgare informazioni sulla struttura e configurazione delle risorse informatiche, con particolare riferimento a quelle che consentono accesso da remoto;
7. accedere senza autorizzazione ai locali server dei plessi, nonché ai locali ed alle aree riservate alle apparecchiature di rete in ciascun plesso e nella sede centrale;
8. intraprendere ogni altra azione diretta a degradare le risorse del sistema, impedire ai soggetti autorizzati l'accesso alle risorse, ottenere risorse superiori a quelle autorizzate o accedere alle risorse informatiche violandone le misure di sicurezza.

Gli Utenti inoltre:

9. sono tenuti ad agire in conformità alla legge e nel rispetto delle indicazioni del Servizio informatico d'Istituto, garantendo la riservatezza nel trattamento dei dati personali, anche mediante la puntuale osservanza delle norme dettate dall'Istituto in materia e rese note con apposite circolari;
A titolo d'esempio:
- non possono servirsi dell'accesso ad internet per attività in violazione del diritto d'autore o di altri diritti tutelati dalla normativa vigente;
- non possono accedere a siti di intrattenimento o di altro genere (pornografici, …) e in ogni caso con finalità diverse da quelle istituzionali;
- inviare fotografie, video, audio, dati personali propri o di amici attraverso le reti informatiche della scuola.
10. nella scelta degli strumenti informatici di cui si servono, devono tenere in opportuna considerazione le indicazioni del Servizio informatico d'istituto, in particolare per quanto riguarda le caratteristiche relative alla sicurezza, privilegiando i sistemi e le procedure che offrono i livelli più elevati di protezione;
11. sono responsabili dei dati e del software che installano sui computer loro affidati: procedono ad una loro attenta valutazione preliminare e non installano software privi delle regolari licenze;
12. sono tenuti a proteggere da accessi non autorizzati i dati utilizzati e/o memorizzati nei propri computer e nei sistemi cui hanno accesso, rispettando in particolare in maniera puntuale le disposizioni sulla cifratura;
13. non possono salvare nelle aree interne di condivisione della rete alcun fine che non sia legato all'attività lavorativa;
14. non possono scaricare, scambiare o utilizzare materiale coperto dal diritto d'autore senza aver acquisito la relativa licenza;
15. non possono utilizzare servizi esterni, ivi inclusi quelli di tipo cloud, senza preventiva autorizzazione del Servizio informatico d'istituto e del Dirigente. Devono comunque prestare la necessaria attenzione all'utilizzo di tali servizi nel rispetto dei principi di sicurezza, conservazione e. se applicabile, confidenzialità dei dati;
16. sono tenuti a proteggere il proprio account mediante password che rispettino gli stessi standard di sicurezza della posta elettronica del dominio @iccarvico.edu.it e, qualora siano presenti più sistemi di autenticazione, differenti per ogni sistema;
17. non devono diffondere né comunicare la propria password, ovvero concedere ad altri l'uso del proprio account;
18. sono tenuti a segnalare immediatamente al Responsabile di plesso e al Servizio informatico d'istituto incidenti, sospetti abusi e violazioni della sicurezza;

19. per i sistemi operativi che lo prevedono, devono utilizzare programmi antivirus aggiornati, avendo cura di sottoporre a scansione antivirus file e programmi scambiati via rete e i supporti rimovibili utilizzati;
20. non devono mantenere connessioni remote inutilizzate né abbandonare la postazione di lavoro con connessioni aperte non protette;
21. sono tenuti, al termine del rapporto di lavoro/collaborazione con l'Istituto a trasferire al proprio responsabile di plesso, o al Dirigente o al soggetto da questo delegato, i file di contenuto inerente l'attività di servizio/collaborazione e a cancellare in via definitiva eventuali altri file. Entro il termine di sei mesi dalla cessazione del rapporto, l'Istituto provvede alla cancellazione dei dati presenti sulle risorse informatiche riferibili all'utente secondo le modalità indicate nel provvedimento del Garante per la tutela dei dati personali del 13 ottobre 2008.
In caso di impossibilità o impedimento dell'Utente, ovvero laddove lo stesso, prima della cessazione del rapporto, non abbia reso disponibili i file attinenti l'attività di servizio/collaborazione e non abbia delegato un collega a inoltrarli, il Dirigente, o un suo delegato, può accedere alle risorse assegnategli per il periodo necessario a recuperare i dati di interesse.
In caso di grave improvvisa indisponibilità o decesso dell'Utente, il Dirigente, su richiesta e previa verifica della compatibilità dell'istanza con la vigente normativa in tema di protezione dei dati personali, potrà rendere disponibile agli aventi diritto i file con contenuti personali.

Utilizzo di dispositivi di proprietà dell'Istituto

L'utente è responsabile del dispositivo portatile di proprietà dell'Istituto che gli venisse assegnato in comodato d'uso gratuito e deve:

1. applicare al dispositivo portatile le regole di utilizzo previste per gli altri dispositivi connessi in rete;
2. custodirlo con diligenza e in luogo protetto durante gli spostamenti;
3. rimuovere gli eventuali files elaborati sullo stesso prima della sua riconsegna.

Agli studenti possono essere assegnati solo dispositivi controllati da un sistema nominativo di gestione delle autenticazioni, previa istanza da parte dei genitori o dell'esercente la responsabilità genitoriale al Dirigente scolastico. I genitori o l'esercente la responsabilità genitoriale sono tenuti a restituire il dispositivo nelle stesse condizioni in cui lo hanno ricevuto al termine del periodo di utilizzo e comunque alla cessazione dell'iscrizione del figlio o della figlia presso l'Istituto.
In caso di danneggiamento o deterioramento del dispositivo al di fuori di quello ordinariamente connesso con l'utilizzo, sono tenuti al risarcimento del danno nei confronti dell'Istituto.

Individuazione e compiti dei Responsabili delle aule informatiche dei plessi

Il Responsabile delle aule informatiche di plesso è individuato dal Dirigente in ragione delle funzioni assegnate e delle competenze possedute, sentito il parere non vincolante del Collegio dei docenti. La designazione è comunicata al Servizio informatico d'istituto.

Il Responsabile delle aule informatiche di plesso:

1. divulga, nell'ambito del proprio plesso, le indicazioni del Servizio informatico d'istituto relative alla sicurezza delle risorse ed al corretto uso delle stesse. Coordina gli utenti e l'uso delle risorse

locali di ciascun plesso, in conformità alle indicazioni del presente disciplinare e dell'Amministratore di sistema;
2. in caso di necessità, fornisce al Servizio informatico d'istituto informazioni o accesso alle risorse informatiche del proprio plesso;
3. svolge compiti di monitoraggio, supporto immediato ai docenti dei plessi, supervisione delle attrezzature delle aule informatiche e delle reti dei plessi;
4. controlla in particolare che sui dispositivi locali siano rispettate le regole in materia di cifratura dei dati e di utilizzo dei file vault;
5. segnala al Servizio informatico d'istituto eventuali dispositivi non protetti da antivirus o non aggiornati;
6. collabora su richiesta alle operazioni di censimento dei dispositivi attivi.

Individuazione e compiti dell'Amministratore di sistema

L'Amministratori di Sistema è unico per tutto l'Istituto ed è designato dagli Enti locali d'intesa con il Dirigente.

L'Amministratore di sistema, oltre all'osservanza di tutte le disposizioni precedenti, è tenuto a:
1. mantenere i sistemi al livello di sicurezza appropriato al loro uso;
2. verificare con regolarità l'integrità dei sistemi;
3. controllare e conservare i log di sistema per il tempo necessario a verificare la conservazione degli standard di sicurezza;
4. segnalare immediatamente ai membri del Servizio informatico d'istituto, sospetti abusi e violazioni della sicurezza e partecipare alla loro gestione;
5. installare e mantenere aggiornati programmi antivirus per i sistemi operativi che lo prevedono;
6. non visionare i dati personali e della corrispondenza di cui dovessero venire a conoscenza e comunque a considerarli strettamente riservati e a non riferire, né duplicare o cedere a persone non autorizzate informazioni sull'esistenza o sul contenuto degli stessi;
7. in caso di interventi di manutenzione, impedire, per quanto possibile, l'accesso alle informazioni e ai dati personali presenti nei sistemi amministrati;
8. seguire attività formative in materie tecnico-gestionali e di sicurezza delle reti, nonché in tema di protezione dei dati personali e di segretezza della corrispondenza.

Compiti del Servizio informatico d'istituto

Il Servizio informatico d'istituto, al fine di mantenere il più elevato livello di sicurezza all'interno delle reti locali, in relazione all'evoluzione tecnologica del settore:
1. controlla che gli accessi remoti alle risorse locali avvengano esclusivamente mediante l'uso di protocolli che prevedano l'autenticazione e la cifratura dei dati trasmessi;
2. limita l'uso interno di servizi e programmi che trasmettono in chiaro le password;
3. sulle macchine gestite, provvede a disattivare i servizi non essenziali ed a limitare il numero degli utenti privilegiati a quello strettamente necessario per le attività di coordinamento, controllo e monitoraggio della rete e dei servizi ad essa afferenti;
4. effettua la revisione, almeno annuale, degli account;
5. effettua il monitoraggio della rete e dei sistemi gestiti, incluse le risorse utilizzate per l'erogazione di servizi di tipo cloud, al fine di garantirne la funzionalità e la sicurezza;
6. realizza i sistemi di filtraggio e logging sugli apparati perimetrali della rete;

7. fornisce supporto per conservare e incrementare la sicurezza delle risorse affidate agli utenti, in particolare trasmette agli utenti le indicazioni e le segnalazioni del Computer Security Incident Response Team del Ministero dell'Istruzione e del Merito (CSIRT MI), accessibili tramite la intranet https://iam.pubblica.istruzione.it/iam-areariservata-web/contenuto/pagina/computer-security-incident-response-team-del-ministero-dell-istruzione-csirt-mi-

Disposizioni per l'uso dei sistemi esterni

Il trattamento dei dati personali di qualunque tipo o di particolare rilevanza per l'Istituto può essere effettuato mediante l'uso di servizi esterni, anche di tipo *cloud*, soltanto ove l'Istituto abbia preventivamente verificato i rischi e i benefici connessi ai servizi offerti, i limiti nella circolazione e trasferimento dei dati, nonché l'affidabilità del fornitore, la sussistenza di garanzie e cautele per la conservazione, persistenza e confidenzialità dei dati oltre ai profili di responsabilità nel trattamento.

Principi generali di tutela dei dati personali

La tutela dei dati personali costituisce un principio fondamentale a cui deve ispirarsi l'azione di tutte le pubbliche amministrazioni e in particolare della scuola. La regolamentazione delle misure di tutela dei dati personali trova oggi la sua fonte nella normativa europea, a partire dal Regolamento (UE) 2016/679 (noto come General Data Protection Regulation, ossia GDPR dal suo acronimo). Nel seguito di questo documento ci si riferirà a tale atto con il termine Regolamento.

Il Regolamento pone un obbligo generalizzato di progettare il trattamento dei dati personali, in special modo attraverso sistemi digitali, nell'intero ciclo di vita, dalla creazione, alla conservazione, trasmissione, elaborazione e cancellazione dei dati.

Si specifica che il riferimento è a **tutti i dati personali**, comunque intesi (e non solo alle categorie particolari di dati - l'origine razziale od etnica, le convinzioni religiose, filosofiche, le opinioni politiche, l'appartenenza sindacale, relativi alla salute o alla vita sessuale, i dati genetici, i dati biometrici e quelli relativi all'orientamento sessuale - e a quelli giudiziari, ossia i c.d. dati sensibili e super-sensibili).

Di conseguenza le istruzioni di questo documento si applicano a qualunque file che contenga dati personali, da intendersi come le informazioni che identificano o rendono identificabile, **direttamente o indirettamente**, una persona fisica e che possono fornire informazioni sulle sue caratteristiche, le sue abitudini, il suo stile di vita, le sue relazioni personali, il suo stato di salute, la sua situazione economica, ecc.

I principi cardine da rispettare sono due: la *privacy by default* e la *privacy by design*. Bisogna cioè progettare i sistemi e applicare regole di condotta e organizzative che **consentano automaticamente (*privacy by default*) e in modo predefinito (*privacy by design*)** di rispettare gli obblighi di tutela dei dati personali posti dal Regolamento.

Le conseguenze del mancato rispetto di tali prescrizioni sono significative. La perdita di controllo su dispositivi contenenti dati personali può comportare, in particolare se i file non sono cifrati, la necessità di aprire una segnalazione al Garante della Privacy da parte del Responsabile della Protezione dei Dati **entro 72 ore dalla scoperta.** Si pensi al caso di furto o smarrimento di un

dispositivo: l'evento deve comunque essere segnalato al Dirigente scolastico, il quale trasmetterà la comunicazione al Responsabile della Protezione dei Dati ai fini della valutazione dell'obbligo di aprire una segnalazione formale di *data breach* al Garante della Privacy. Uno degli elementi più importanti nella valutazione della correttezza del trattamento dei dati da parte dell'Istituto e dei suoi docenti e del personale scolastico in generale è proprio l'applicazione delle misure di cifratura, oltre all'adeguatezza delle misure di sicurezza e di protezione degli accessi.

Disposizioni di tutela dei dati personali sui dispositivi locali e sui sistemi cloud

L'Istituto adotta le seguenti misure ai fini della tutela dei dati personali sui dispositivi locali e sui sistemi cloud, distinte in misure di tipo tecnico e in misure di tipo organizzativo.

Misure di tipo tecnico di protezione dei dati

1. Qualunque file contenente dati personali **deve essere salvato sui dispositivi locali solo ed esclusivamente previa cifratura.**
2. Nessun file contenente dati personali deve restare sui dispositivi locali dell'Istituto se non inserito all'interno di un file vault.
3. **Inserimento di chiavette USB**
   a) Non si possono utilizzare chiavette USB contenenti file con dati personali se non inseriti all'interno di una cassaforte. I docenti di sostegno devono utilizzare le chiavette USB cifrate consegnate già predisposte con i sistemi di cifratura da parte delle funzioni strumentali per l'inclusione.
   b) Dopo l'apertura della cassaforte, l'unità logica così creata deve essere sottoposta a scansione antivirus.
4. Verifica dello stato di sicurezza dei dispositivi
   Semestralmente i responsabili delle aule informatiche segnaleranno al Sistema informativo d'istituto eventuali dispositivi privi di antivirus aggiornato e lo stato degli aggiornamenti del sistema operativo.
5. **Cancellazione dei dati al termine del ciclo di vita di un dispositivo**
   Quando un dispositivo non è più utilizzabile e deve essere dismesso, previa autorizzazione del Direttore dei Servizi Generali e Amministrativi responsabile dello scarico inventariale:

   i) il responsabile dell'aula informatica o l'animatore digitale, con il supporto se necessario dell'assistente tecnico, provvede **alla formattazione sicura dei dispositivi di storage** (hard disk, …)
   Per gli altri sistemi operativi deve essere richiesto l'intervento dell'assistente tecnico.

   ii) successivamente a tale operazione, il dispositivo può essere dismesso contattando gli uffici di segreteria che si occuperanno dello smaltimento a norma.
6. Gli utenti devono comunque provvedere (almeno ogni sei mesi) alla pulizia dei file vault, con cancellazione dei file inutili per evitare archiviazioni non necessarie.

Misure organizzative di protezione dei dati

1. Il rinvenimento di qualunque file contenente dati personali al di fuori delle casseforti (file vault) su dispositivi locali dell'Istituto espone a responsabilità il suo autore o il suo

modificatore. In ogni caso il file sarà immediatamente cancellato previo avviso al responsabile di sede da parte di chi ha individuato il file, **senza notifica al suo autore o modificatore.**

2. Creazione delle casseforti di plesso, di modulo, di docente e di consiglio di classe

   Le casseforti (file vault) sono a tutti gli effetti l'analogo digitale del cassetto della cattedra e del cassetto del professore, dei consigli di classe, del plesso, … del mondo analogico basato sui documenti cartacei.

   Saranno attivati da parte dei responsabili delle aule informatiche, dell'animatore digitale e dei coordinatori di classe:
   - i) un file vault per ciascun consiglio di classe e per ciascun modulo della scuola primaria;
   - ii) un file vault di plesso.

   Le **password** dei singoli file vault saranno **consegnate a tutti i docenti interessati**, le **chiavi dei file vault** dovranno essere inoltrate a luigi.valsecchi@iccarvico.edu.it ai fini dell'archiviazione nella sezione riservata sul sistema di gestione documentale della scuola.

   Qualunque documento digitale riferito alla classe dovrà essere conservato esclusivamente entro tali file vault.

Misure organizzative specifiche per la posta elettronica

Gli utenti sono responsabili del corretto utilizzo delle caselle di posta elettronica sui domini @iccarvico.edu.it e @iccarvico.it e sono tenuti ad utilizzarle in modo conforme a quanto stabilito dal presente disciplinare. Oltre alle istruzioni fornite negli altri paragrafi del presente disciplinare, si richiamano i seguenti obblighi.
Gli utenti devono:

1. conservare la password nella massima riservatezza e con la massima diligenza;
2. mantenere la casella in ordine, cancellando documenti inutili e allegati ingombranti;
3. utilizzare tecniche per l'invio di comunicazione a liste di distribuzione solo se istituzionali;
4. utilizzare la ricevuta di ritorno per avere la conferma dell'avvenuta lettura del messaggio da parte del destinatario;
5. accertarsi dell'identità del mittente e controllare con i software antivirus i file in allegato ai messaggi di posta elettronica;
6. rispondere a email pervenute da mittenti conosciuti e cancellare preventivamente le altre;
7. non aprire link contenuti all'interno dei messaggi se non si ha la comprovata sicurezza sul contenuto delle pagine richiamate.

Agli utenti è fatto espresso divieto di qualsiasi uso della posta elettronica che possa in qualche modo recare danno all'istituto o a terzi e quindi di:

1. utilizzare strumenti software o hardware atti ad intercettare il contenuto delle comunicazioni informatiche all'interno dell'istituto;
2. trasmettere a mezzo posta elettronica dati sensibili, personali o commerciali di alcun genere se non nel rispetto delle norme sulla disciplina del trattamento della protezione dei dati;
3. inviare tramite posta elettronica user-id, password, configurazioni della rete interna, indirizzi e nomi dei sistemi informatici;

4. utilizzare le caselle di posta elettronica per l'invio di messaggi personali o per la partecipazione a dibattiti, forum o mailing-list salvo diversa ed esplicita autorizzazione;

Misure specifiche per dispositivi personali (BYOD)

L'utilizzo dei dispositivi personali da parte degli studenti è in linea generale vietato. Specifiche autorizzazioni possono essere concesse dal Dirigente scolastico in presenza di motivazioni adeguate (ad es. con riferimento all'utilizzo di software di ausilio per Disturbi Specifici di Apprendimento).
In ogni caso l'utilizzo di dispositivi personali è soggetto alla preventiva acquisizione di una liberatoria da parte del genitore ovvero dell'esercente la responsabilità genitoriale di esclusione di ogni responsabilità in capo all'Istituto e al suo personale derivante da utilizzo illecito ovvero da furto, danneggiamento, distruzione del dispositivo personale.

Utilizzo di telefonini ed altre apparecchiature di registrazione di immagini e suoni

È fatto divieto assoluto di effettuare riprese, fotografie, registrazioni di suoni con qualsiasi tipologia di apparecchiatura elettronica adatta a tali scopi, salvo:

1. diversa disposizione esplicita del Dirigente, da concordarsi di volta in volta e comunque sempre preventivamente al trattamento;
2. informazione preventiva agli interessati;
3. acquisizione del loro libero consenso, preventivo ed informato.

Regole di utilizzo delle aule informatiche e delle aule speciali

Utilizzo dei PC e degli altri dispositivi

Gli utenti sono tenuti a:

1. attivare sui PC screen saver e relativa password;
2. conservare la password nella massima riservatezza e diligenza;
3. non inserire password locali che non rendano accessibili il computer agli amministratori di rete se non esplicitamente autorizzato dall'amministratore di sistema;
4. non utilizzare criptosistemi o qualsiasi altro programma di sicurezza crittografica non previste esplicitamente dal servizio informatico dell'istituto;
5. non modificare la configurazione hardware e software del proprio PC, se non esplicitamente autorizzati dal servizio informatico dell'istituto;
6. non rimuovere, danneggiare o asportare componenti hardware;
7. non installare sul proprio PC dispositivi hardware personali (modem, schede audio, masterizzatori, dischi esterni, …), salvo specifica autorizzazione in tal senso da parte del servizio informatico dell'istituto;
8. non installare autonomamente programmi informatici, se non esplicitamente autorizzati dal servizio informatico dell'istituto;
9. non utilizzare programmi non autorizzati, con particolare riferimento ai videogiochi o app;
10. mantenere sempre aggiornati e attivi sulla propria postazione di lavoro i software antivirus con riferimento all'ultima versione disponibile;
11. nel caso il software antivirus rilevi la presenza di un virus, sospendere immediatamente ogni elaborazione in corso senza spegnere il computer e segnalare prontamente l'accaduto al servizio informatico dell'istituto;

12. prestare la massima attenzione ai supporti di origine esterna (es. pen drive), verificando preventivamente tramite il programma antivirus ogni file acquisito attraverso qualsiasi supporto e avvertendo immediatamente il servizio informatico dell'istituto nel caso vengano rilevati virus o eventuali malfunzionamenti;
13. non lasciare incustodita ed accessibile la propria postazione una volta connesso al sistema con le proprie credenziali di autenticazione;
14. non cedere, una volta superata la fase di autenticazione, l'uso della propria stazione a persone non autorizzate, in particolar modo per quanto riguardo l'accesso a internet, al registro elettronico, ai servizi di posta elettronica e ai sistemi di condivisione;
15. spegnere il PC al termine del lavoro o in caso di assenze prolungate dalla propria postazione.

Utilizzo delle stampanti e dei materiali di consumo

Stampanti e materiali di consumo in genere (carta, inchiostro, toner, supporti digitali, filamenti delle stampanti 3D, …) possono essere usati esclusivamente per compiti di natura strettamente istituzionale, evitando in ogni modo sprechi e utilizzi eccessivi.
Gli utenti devono effettuare la stampa dei dati solo se strettamente necessaria e ritirare prontamente dai vassoi delle stampanti comuni i fogli per impedire a persone non autorizzate di accedere alle stampe di documenti riservati.
Gli utenti devono distruggere personalmente e sistematicamente le stampe non più necessarie.

Utilizzo dei sistemi di realtà aumentata e realtà virtuale

I sistemi di realtà aumentata e realtà virtuale si caratterizzano la convergenza fra realtà fisica e virtuale nell'esperienza di apprendimento. In linea di principio, i sistemi di realtà aumentata e virtuale mirano ad un'esperienza che unisce il mondo fisico a quelle virtuale con una progressiva assimilazione delle modalità di accesso e di fruizione dei due mondi.
L'utilizzo in ambito scolastico di queste tecnologie richiede il rispetto di alcune regole generali di tipo precauzionale:

1. I sistemi di realtà aumentata e realtà virtuale (sistemi AR-VR) possono essere usati esclusivamente nelle aree che saranno all'uopo attrezzate;
2. Cappotti, contenitori, borse e altri oggetti voluminosi non possono essere introdotti all'interno dell'area dei sistemi AR-VR;
3. Il numero massimo di utenti ammissibile all'interno dell'area dei sistemi AR-VR è specificato all'ingresso del locale e non deve essere mai superato;
4. Ciascun utente all'interno dell'area dei sistemi AR-VR deve sempre mantenere libere entrambe le mani;
5. L'utilizzo dei deve avvenire in modo da evitare l'esposizione a rischi, e con prudenza e cautela, al fine di evitare situazioni di pericolo per sé o altri, secondo le specifiche regole fornite per ogni attività AR-VR.

Trattamento dei dati acquisiti in relazione all'uso delle risorse informatiche e all'accesso ali servizi di rete

L'Istituto, nel rispetto dei principi di libertà e dignità, non consente l'installazione di strumentazioni hardware e software mirate al controllo degli utenti e vieta il trattamento effettuato mediante apparecchiature preordinate al controllo a distanza quali:
a) la lettura e la registrazione sistematica dei messaggi di posta elettronica, al di là di quanto necessario per svolgere il servizio di posta elettronica;
b) la riproduzione ed eventuale memorizzazione sistematica delle pagine web visualizzate dall'utente;
c) la lettura e registrazione dei caratteri inseriti tramite tastiera o dispositivi analoghi;
d) l'analisi occulta di computer portatili affidati in uso.

Con riferimento all'accesso alla rete, il Servizio informatico d'istituto, per le finalità indicate al punto successivo raccoglie le informazioni relative all'associazione tra indirizzo, nome del computer e utente; non registra il contenuto delle connessioni, può raccogliere tuttavia alcune informazioni relative alle transazioni eseguite quali: indirizzi dei nodi, ora di inizio e fine transazione e quantità dei dati trasferiti.

I dati di cui al paragrafo precedente sono conservati per un periodo non superiore a un anno e sono utilizzabili dal personale del Servizio informatico d'istituto competente solamente con fini di controllo della sicurezza e per l'ottimizzazione dei sistemi. Le Strutture in cui sono installati proxy server o altri sistemi di controllo delle sessioni possono conservare i file di log contenenti informazioni relative alle pagine web, interne od esterne, accedute dai nodi locali. Tali informazioni, conservate per un periodo non superiore a un mese a cura del Servizio informatico d'istituto, sono esaminate o elaborate soltanto ove si ravvisi la necessità di garantire la sicurezza o il buon funzionamento del sistema.

Raccolta di dati in relazione al servizio di posta elettronica

Il Servizio informatico d'istituto, per esigenze organizzative connesse al funzionamento, sicurezza e salvaguardia del servizio di posta elettronica, può richiedere al fornitore del servizio data, ora, indirizzi del mittente e del destinatario dei messaggi di posta, nonché il risultato delle analisi dei software antivirus ed antispam.
I dati eventualmente registrati dal fornitore, utilizzati anche per elaborazioni statistiche, sono conservati secondo le regole e i tempi previsti dal fornitore in conformità alle vigenti normative a tutela dei dati personali. Essi sono accessibili dal solo personale, appositamente incaricato, del Servizio informatico d'istituto.
L'istituto non effettua copie di salvataggio dei messaggi di posta elettronica personale. L'istituto può rendere disponibili indirizzi di posta elettronica condivisi all'interno del dominio attraverso l'uso di liste di distribuzione di e-mail, nonché messaggi di risposta automatica, in caso di assenza programmata dei titolari.
La casella di posta elettronica è disattivata entro i sei mesi successivi alla scadenza del termine nel quale l'utente è stato autorizzato all'accesso. Entro tale periodo l'utente ha il dovere di trasferire al Dirigente o a un suo delegato le comunicazioni di servizio d'interesse e di trasmettergli quelle nel frattempo intervenute. Il contenuto della casella è comunque cancellato entro un anno dalla scadenza del termine di autorizzazione all'accesso. I periodi indicati nel presente capoverso possono essere prolungati dal Dirigente ove ne ravvisi specifica esigenza. In caso di impossibilità o

impedimento del titolare della casella di posta elettronica, il Dirigente o un suo delegato può avere accesso alla casella per un periodo non superiore a un mese dalla data di conoscenza della situazione che ha determinato l'impossibilità o l'impedimento.

Ulteriori misure per la tutela dei sistemi informativi

Al fine di assicurare la funzionalità, disponibilità, ottimizzazione, sicurezza ed integrità dei sistemi informativi e prevenire utilizzazioni indebite, l'Istituto adotta misure che consentono la verifica di comportamenti anomali o delle condotte non previste dal presente Disciplinare nel rispetto dei principi generali di necessità, pertinenza e non eccedenza sopra richiamati.
A tal fine il Servizio informatico d'istituto può eseguire elaborazioni sui dati registrati dirette ad evidenziare anomalie nel traffico di rete o condotte non consentite dal presente Disciplinare.
Nel caso in cui, nonostante l'adozione di accorgimenti tecnici preventivi, si verifichino eventi dannosi o rilevino comportamenti anomali o non consentiti, il Servizio informatico d'istituto esegue, previa informazione agli interessati e salvo i casi di necessità ed urgenza, ulteriori accertamenti e adotta le misure necessarie ad interrompere le condotte dannose o non consentite.
Nei casi di reiterazione di comportamenti vietati e già segnalati o di particolare gravità, l'animatore digitale e l'amministratore di sistema adotta tutte le misure tecniche necessarie, dandone immediata comunicazione al Dirigente, che dispone gli ulteriori provvedimenti ai sensi del punto seguente.
Il Dirigente, in relazione alle funzioni a lui assegnate circa il trattamento dei dati personali, adotta ogni opportuna misura affinché i soggetti preposti al trattamento dei dati relativi all'uso di internet e della posta elettronica svolgano soltanto le operazioni strettamente necessarie al perseguimento delle relative finalità, senza realizzare attività di controllo a distanza, neppure di propria iniziativa
In caso di comportamento illecito o di abuso dell'utilizzo delle risorse informatiche e delle reti d'istituto, il Dirigente valuta i profili di responsabilità disciplinare dei dipendenti e degli studenti ai fini del seguito di competenza, fatta salva la segnalazione all'autorità giudiziaria qualora i comportamenti o gli atti posti in essere integrino ipotesi di reato.

Sorveglianza e monitoraggio

La corretta applicazione delle regole del presente disciplinare è affidata alla sorveglianza del Direttore dei Servizi Generali e Amministrativi per il personale ATA e al responsabile delle aule informatiche di ciascun plesso, coadiuvato dal responsabile di sede, per i docenti e i dispositivi nei plessi.
Il monitoraggio dell'applicazione delle regole del presente disciplinare è realizzato, per i profili di competenza, dal Servizio informatico d'istituto.
Il datore di lavoro, per esigenze organizzative, per garantire la sicurezza sul lavoro, per evitare reiterati comportamenti dolosi e illeciti può avvalersi legittimamente, nel rispetto dell'articolo 4 comma 2 dello Statuto dei lavoratori, di sistemi che consentano un controllo a distanza e determinano il trattamento di dati personali riferibili a singoli utenti.
Il datore di lavoro non può in alcun caso utilizzare detti sistemi per ricostruire l'attività del lavoratore tramite

- lettura e registrazione sistematica di messaggi di posta elettronica, al di là di quanto necessario per fornire e gestire il servizio di posta elettronica stesso;
- memorizzazione sistematica delle pagine web visualizzate;
- lettura e registrazione dei caratteri inseriti dal lavoratore tramite tastiera o dispositivi analoghi;

- analisi occulta dei dispositivi per l'accesso a internet o alla posta elettronica messi a disposizione dei dipendenti.

Le attività sull'uso del servizio di accesso ad internet vengono automaticamente registrate attraverso il log di sistema ottenuti da un proxy server o da altro strumento di registrazione delle informazioni. Analogamente sono parimenti suscettibili di controllo i servizi di posta elettronica. Tali file possono essere messi a disposizione dell'autorità giudiziaria in caso di accertata violazione della normativa vigente.

I dati contenuti nei log sono conservati per il tempo strettamente necessario al perseguimento di finalità organizzative, produttive di verifica della funzionalità dei sistemi di protezione.

La riservatezza delle informazioni registrate è soggetta a quanto dettato dal Regolamento (UE) 2016/679 e dal D.Lgs. n. 196/2003 e ss.mm.ii., il trattamento dei dati avviene esclusivamente per fini istituzionali, per attività di monitoraggio e controllo e in forma anonima in modo tale da precludere l'identificazione degli utenti o delle loro attività.

Le registrazioni possono essere utilizzate per fornire informazioni esclusivamente su:

- numero di utenti che visita ciascun sito o dominio, numero di pagine richieste e quantità dati scaricati;
- numero dei siti visitati da ciascun utente, quantità totale di dati scaricati, postazioni di lavoro utilizzate per la navigazione.

I dati personali contenuti nei log possono essere trattati tassativamente solo nelle seguenti ipotesi:

- per corrispondere ad eventuali richieste dell'autorità giudiziaria e della polizia postale;
- quando si verifichi un evento dannoso o una situazione di pericolo che richiede un immediato intervento;
- in caso di utilizzo anomalo degli strumenti da parte degli utenti reiterato nonostante l'esplicito invito ad attenersi alle istruzioni impartite.

Qualora i controlli evidenzino un utilizzo anomalo degli strumenti informatici dell'istituto, il Dirigente procede in forma graduata :

- in via preliminare si eseguono controlli su dati aggregati, in forma anonima e si provvede ad un avviso generalizzato agli utenti;
- se perdurano le anomalie si procede a controlli per tipologie di locali di utilizzo (uffici, aule, etc.) o tipologie di utenti (ATA, docenti, studenti) e si procede con avvisi mirati alle categorie di utilizzatori;
- ripetendosi l'anomalia, sarà lecito il controllo su base individuale e si procederà all'invio di avvisi individuali;
- in caso di verificato e reiterato uso non conforme delle risorse informatiche il titolare del trattamento attiva il procedimento disciplinare.

Nel caso di esplicite segnalazioni o denunce di utilizzo improprio delle attrezzature informatiche, degli accessi a internet o dell'utilizzo della posta elettronica, il Dirigente, avvalendosi del Servizio informatico d'istituto, è tenuto ad effettuare controlli su base individuale per accertare la fondatezza o meno delle segnalazioni. i detti controlli dovrà essere data comunicazione all'utente interessato.

Violazione delle norme

Ogni condotta posta in essere in violazione del presente Disciplinare potrà determinare la sospensione dell'accesso alle risorse informatiche e ai servizi di rete, salvo eventuali azioni disciplinari, civili o penali. La violazione delle disposizioni del presente Disciplinare che cagioni a terzi un danno risarcito dall'Istituto potrà determinare, nei confronti del responsabile, l'esercizio del diritto di rivalsa nelle forme e nei limiti stabiliti dalla legge.

Informativa

Il presente Disciplinare costituisce informativa ai sensi dell'art. 4, c. 3, della legge 20 maggio 1970 n.300 e s.m.i. circa le modalità e finalità del trattamento dei dati personali connessi all'uso delle risorse informatiche e dei servizi di rete. L'Istituto assicura al presente Disciplinare e ai suoi successivi aggiornamenti la più ampia diffusione presso gli utenti mediante pubblicazione nel sito istituzionale della scuola, nonché consegnandolo a ciascuno in modalità elettroniche o cartacee, idonee comunque a dimostrare l'avvenuta consegna.
Il presente Disciplinare abroga e sostituisce integralmente tutti i precedenti regolamenti adottati in materia.

Clausola di revisione

Il presente Disciplinare è aggiornato periodicamente in relazione all'evoluzione della tecnologia e della normativa di settore.

Allegati

Regole tecniche di cifratura

1. **La creazione di una cassaforte (file vault)** avviene con il software open source Cryptomator.
2. Si fa riferimento alla Guida alla creazione di File Vault (cassaforti per file) – data ultima revisione: 21 dicembre 2022
3. La cifratura dei singoli file avviene secondo le metodologie riassunte nella Guida alla cifratura dei file – data ultima revisione: 21 dicembre 2022.

Regole tecniche di formattazione sicura

1. Si fa riferimento agli standard tecnologici maggiormente accreditati e alle raccomandazioni emanate dalle autorità nazionali di protezione dati dell'Unione Europea.
2. I sistemi formattati non possono comunque in nessun caso essere rivenduti all'esterno o comunque smaltiti senza la previa asseverazione della conformità della procedura di formattazione e cancellazione sicura da parte dell'Amministratore di sistema.