Ministero dell'Istruzione
I S T I T U T O C O M P R E N S I V O S T A T A L E "A. M A N Z O N I"

Via dei Platani, 5 - 21053 Castellanza
Tel. 0331/50.42.33 – Fax 0331/50.26.88
Email: vaic81700p@istruzione.it - vaic81700p@pec.istruzione
C.F. 81009410127 - CODICE MECCANOGRAFICO vaic 81700p

Disciplinare per il corretto utilizzo dei sistemi e degli strumenti informatici e telematici, della posta elettronica e della navigazione Internet

Approvato dal Consiglio di Istituto con delibera nr. 88 del 08/07/2024

Indice

Via dei Platani, 5 - 21053 Castellanza
Tel. 0331/50.42.33 – Fax 0331/50.26.88
Email: vaic81700p@istruzione.it - vaic81700p@pec.istruzione
C.F. 81009410127 - CODICE MECCANOGRAFICO vaic 81700p

Capo I - Disposizioni generali

Art.1 Finalità generali

La crescente diffusione delle nuove tecnologie informatiche e, in particolare, il libero accesso alla rete internet dai personal computer, presta il fianco a possibili rischi per la sicurezza informatica delle risorse ICT (Information and Communication Technology) dell'Istituto comprensivo, derivanti anche da un inappropriato utilizzo degli strumenti informatici e telematici messi a disposizione dall'Istituto comprensivo.
Al fine di ridurre il livello di rischio e la probabilità che questo si verifichi, con conseguenti possibili danni patrimoniali, anche di immagine, il presente disciplinare pone le regole per un corretto utilizzo dei sistemi e degli strumenti informatici e telematici, della posta elettronica e della navigazione Internet.

Art.2 Definizioni

Amministratori di sistema: figure professionali finalizzate alla gestione e alla manutenzione di un sistema di elaborazione o di sue componenti o figure equiparabili, quali gli amministratori di basi di dati, gli amministratori di reti e di apparati di sicurezza e gli amministratori di sistemi software complessi

Anonimizzazione dei dati: l'anonimizzazione rende impossibile l'identificazione dell'utente, di conseguenza i dati anonimizzati non sono soggetti alle restrizioni sul trattamento dei dati personali ai sensi del Regolamento generale sulla protezione dei dati. Bisogna fare attenzione a non confondere la pseudonimizzazione con l'anonimizzazione. Si tratta, infatti, di due concetti solo in apparenza simili, ma che hanno un significato diverso. Un dato pseudonimizzato, infatti, non elimina il rischio che lo stesso possa essere ricostruito e riassociato all'utente. Quindi non fa venire meno il presupposto di identificabilità che rende applicabile la disciplina GDPR. Le principali tecniche di anonimizzazione dei dati sono 4:

- Mascheramento: consiste nell'eliminazione degli identificatori personali e diretti, come ad esempio nome e indirizzo, agendo quindi sul livello di dettaglio del dato e senza alterare o modificare i dati originali.
- Randomizzazione: è una famiglia di tecniche che prevedono l'alterazione dei dati di partenza con l'obiettivo di spezzare il legame tra questi e l'individuo di riferimento. Fanno parte di questo gruppo tecniche come il rumore statistico (modifica dei dati attraverso l'aggiunta di piccoli cambiamenti casuali) e la permutazione (vengono mescolati i valori presenti in una tabella in modo che non sia più possibile ricostruire l'associazione originale tra i dati).
- Generalizzazione dei dati: questo tipo di tecniche modificano la scala o l'ordine di grandezza – ad esempio indicando una provincia invece di una città – in modo che sia meno probabile riconoscere soggetti precisi, poiché è plausibile che più persone condividano gli stessi valori. Una delle tecniche di generalizzazione più utilizzate è la k-anonimizzazione (ogni valore relativo a un interessato deve essere condiviso da un numero minimo k di altri interessati che fanno parte dell'insieme);
- Anonimizzazione stratificata: detta anche ri-anonimizzazione, consiste in una seconda anonimizzazione di dati già resi anonimi in una fase precedente.

Applicazioni istituzionali: si considerano applicazioni istituzionali:

- Prodotti/programma acquistati dall'amministrazione, di valenza generale o settoriale ed in quest'ultimo caso approvati dai sistemi informativi;
- Applicazioni e servizio sviluppate ad hoc dai sistemi informativi, da terze parti ma sotto il coordinamento dei sistemi informativi ovvero da altre strutture con un processo di partecipazione e approvazione da parte dei sistemi informativi e che seguono le regole di gestione previste nei casi precedenti;

Via dei Platani, 5 - 21053 Castellanza
Tel. 0331/50.42.33 – Fax 0331/50.26.88
Email: vaic81700p@istruzione.it - vaic81700p@pec.istruzione
C.F. 81009410127 - CODICE MECCANOGRAFICO vaic 81700p

- Applicazioni esterne che l'amministrazione utilizza secondo le regole di gestione e di sicurezza delle medesime a titolo di mero esempio possono essere la piattaforma NoiPA, abbonamenti a servizi informativi, portale ANAC, etc.

Backup: duplicazione di un file o di un insieme di file su un supporto esterno al computer, per avere una copia di riserva.

Chat: servizio offerto da Internet, che permette mediante apposito software una 'conversazione' fra più interlocutori costituita da uno scambio di messaggi scritti che appaiono in tempo reale sul monitor di ciascun partecipante.

Chiave USB: o unità flash USB o penna USB (anche in inglese USB flash drive, o pendrive) è una memoria di massa portatile di dimensioni molto contenute che si collega al computer mediante la porta USB.

Client: Computer o programma collegato ad un altro (computer o programma) a cui inoltra le richieste dell'Utente.

Cloud: sistema configurato su server remoto che consente di disporre di risorse software e hardware (come memorie di massa per l'archiviazione di dati, o applicazioni), il cui utilizzo è erogato come servizio.

Criptazione dei dati: tecnica di rappresentazione di un messaggio in una forma tale che l'informazione in esso contenuta possa essere recepita solo dal destinatario. ciò si può ottenere con due diversi metodi: celando l'esistenza stessa del messaggio o sottoponendo il testo del messaggio a trasformazioni che lo rendano incomprensibile. E' possibile utilizzare il software 7-ZIP per proteggere la decrittazione con una password. La prima azione da fare è selezionare i file e le cartelle da crittografare e comprimere. Poi cliccare il pulsante Aggiungi e nella sezione Crittografia inserire una password nello slot Inserisci password per poi confermarla digitandola di nuovo nello slot "Reinserisci password".

Dati: l'insieme di informazioni di cui un Utente, come sotto identificato, viene a conoscenza e di cui deve garantire la riservatezza e la segretezza.

Dati personali: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale (art. 4 GDPR).

Dipendente: personale dell'Ente assunto con qualsiasi tipo di forma contrattuale, anche in stage o tirocinio;

Dispositivi mobili: apparecchi di telecomunicazione portatili (tablet, smartphone, etc.);

Download, scaricamento: ricevere o prelevare tramite rete telematica (ad esempio da un sito web) uno o più file, trasferendolo sul disco rigido del computer o su altra periferica.

File di log: registrazioni sequenziali e cronologiche delle operazioni effettuate da un sistema informativo, necessarie per la risoluzione di problemi ed errori; tali operazioni possono essere effettuate da un Utente oppure avvenire in modo totalmente automatizzato;

File sharing: sistema per lo scambio di file tra utenti di Internet tramite un server comune.

Hard disk: principale unità di memorizzazione dei dati sul computer, in cui vengono memorizzati il sistema operativo, i programmi applicativi, i dati di configurazione del computer, ed eventualmente i documenti creati dall'utente.

Instant messaging: strumenti di comunicazione on-line, simultanea ed in tempo reale, tra due o più utenti.

Via dei Platani, 5 - 21053 Castellanza
Tel. 0331/50.42.33 – Fax 0331/50.26.88
Email: vaic81700p@istruzione.it - vaic81700p@pec.istruzione
C.F. 81009410127 - CODICE MECCANOGRAFICO vaic 81700p

GDPR: General Data Protection Regulation - Regolamento Generale sulla Protezione dei Dati - Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016

LAN: è l'acronimo del termine inglese Local Area Network, (in italiano rete locale). Identifica una rete costituita da computer collegati tra loro, dalle interconnessioni e dalle periferiche condivise in un ambito fisico delimitato.

Login: procedura di accesso a un sistema informatico, che prevede l'inserimento di un codice identificativo (UserID o nome utente) e di una parola d'ordine (Password) da parte dell'utente. Nei sistemi che richiedono particolari cautele di sicurezza può essere integrata con un codice (PIN), assegnato all'utente o rilasciato in tempo reale tramite telefono cellulare (OTP).

Logout: procedura di scollegamento da un sistema informatico a cui si era avuto accesso tramite un'operazione di login.

Malware: abbreviazione per malicious software (che significa letteralmente software malintenzionato, ma di solito tradotto come software dannoso), indica un qualsiasi programma informatico usato per disturbare le operazioni svolte da un computer

Password: parola d'ordine dell'utente.

Phishing: Truffa informatica effettuata inviando un'e-mail con il logo contraffatto di un istituto di credito o di una società di commercio elettronico, in cui si invita il destinatario a fornire dati riservati (numero di carta di credito, password di accesso al servizio di home banking, ecc.), motivando tale richiesta con ragioni di ordine tecnico.

Pila software: elenco di software installati o installabili sui dispositivi istituzionali dell'Istituto comprensivo;

PIN: codice alfanumerico breve (di solito non più di 8 caratteri) abbinato a nome utente e password, che integra la sicurezza negli accessi ai sistemi informatici.

Postazione di lavoro (PdL): personal computer (desktop o portatile) messo a disposizione dall'Istituto comprensivo a ciascun Utente per l'espletamento dell'attività lavorativa;

OTP: codice numerico di sicurezza per accesso ai sistemi informatici, abbinato a nome utente e password, come il PIN, ma rilasciato tramite app o SMS sul telefono cellulare dell'utente, ed utilizzabile una sola volta per un tempo limitato. Server: computer di elevate prestazioni, che in una rete distribuisce un servizio (un applicativo, o l'accesso a cartelle e file di dati) agli elaboratori degli utenti collegati, detti client.

Ransomware: è un tipo di malware che limita l'accesso del dispositivo che infetta, richiedendo un riscatto (ransom in Inglese) da pagare per rimuovere la limitazione

Repository: in un repository sono raccolti dati e informazioni in formato digitale, valorizzati e archiviati sulla base di metadati che ne permettono la rapida individuazione, anche grazie alla creazione di tabelle relazionali. Grazie alla sua peculiare architettura, un repository consente di gestire in modo ottimale anche grandi volumi di dati.
Server: computer denominato servente o programma a cui altri (computer o programmi) si collegano per l'elaborazione delle richieste dell'Utente.

Software: è l'insieme delle componenti immateriali di un sistema informatico, costituito principalmente dai programmi che vengono elaborati dal computer; è contrapposto all'hardware, cioè la parte materiale, tangibile, dello stesso sistema.

SPAM: messaggio pubblicitario non richiesto, inviato in modo massivo e ripetuto a un numero molto

Via dei Platani, 5 - 21053 Castellanza
Tel. 0331/50.42.33 – Fax 0331/50.26.88
Email: vaic81700p@istruzione.it - vaic81700p@pec.istruzione
C.F. 81009410127 - CODICE MECCANOGRAFICO vaic 81700p

Strumento informatico/telematico: personal computer fissi o portatili, stampanti locali o di rete, programmi e prodotti software, apparecchiature adoperate per la comunicazione unificata (videoconferenza, telefonia fissa e mobile, chat, messaggistica generica, social network, posta elettronica, condivisioni, accessi remoti, etc);

Utenti: personale dipendente, personale comandato da altre pubbliche amministrazioni, collaboratori, consulenti, tirocinanti, stagisti, fornitori esterni, coloro che, in virtù di un rapporto di lavoro in essere a qualsiasi titolo con l'Istituto comprensivo, siano autorizzati all'utilizzo degli strumenti informatici messi a disposizione dall'Istituto comprensivo.

Upload: è il processo di invio di un file (o più genericamente di un flusso finito di dati o informazioni) ad un sistema remoto attraverso una rete informatica.

Virus: programma appartenente alla categoria dei malware che, una volta eseguito, infetta dei file in modo da arrecare danni al sistema, rallentando o rendendo inutilizzabile il dispositivo infetto.

Art. 2 Contesto normativo e regolamentare

Il presente disciplinare è redatto sulla base dei seguenti e principali riferimenti normativi e regolamentari:

- Codice penale, con particolare riferimento ai reati informatici;
- Codice civile, con particolare riferimento agli artt. 2104 e 2105;
- L. 300/1970 (Statuto dei lavoratori) - artt. 4, 7 e 8;
- D. Lgs. 196/2003 e s.m.i (Codice in materia di protezione dei dati personali);
- D. Lgs. 82/2005 e s.m.i. (Codice dell'amministrazione digitale);
- Provvedimenti del Garante per la protezione dei dati personali applicabili al contesto oggetto del presente documento, fra cui le "Linee guida per posta elettronica e Internet" di cui alla deliberazione 13/2007;
- D. Lgs. 81/2008 e s.m.i (Testo Unico sulla sicurezza);
- D.P.R 62/2013 (Codice di comportamento dei dipendenti della pubblica amministrazione) e Codice di comportamento del personale docente e non docente dell'Istituto comprensivo;
- Regolamento (UE) 2016/679 (General Data Protection Regulation, di seguito GDPR)
- Direttiva n. 2 del 26 maggio 2009 del Dipartimento della Funzione Pubblica;
- "Linee guida del Garante per posta elettronica e internet" delibera n. 13 del 1 marzo 2007- documento web n. 1387522;
- D.Lgs. 27 ottobre 2009, n. 150, Attuazione della legge 4 marzo 2009, n. 15, in materia di ottimizzazione della produttività del lavoro pubblico e di efficienza e trasparenza delle pubbliche amministrazioni;
- D.lgs. n. 151/2015 (c.d. Jobs Act), art. 23;
- Codice disciplinare e codice di condotta pubblicato sul sito web dell'Istituto comprensivo Manzoni, raggiungibile all'indirizzo web https://istitutocomprensivocastellanza.edu.it/ nella sezione "Le carte della scuola" ed in Amministrazione trasparente, sezione Disposizioni generali > Atti generali > Codice disciplinare e codice di condotta;
- Informative ed autorizzazioni al trattamento dati notificati al personale scolastico ed all'utenza con circolare annuale e pubblicati nella sezione "Le carte della scuola", sottosezione "Politica, organizzazione e Documentazione Privacy" del sito web istituzionale raggiungibile all'indirizzo web https://istitutocomprensivocastellanza.edu.it/ ;

Via dei Platani, 5 - 21053 Castellanza
Tel. 0331/50.42.33 – Fax 0331/50.26.88
Email: vaic81700p@istruzione.it - vaic81700p@pec.istruzione
C.F. 81009410127 - CODICE MECCANOGRAFICO vaic 81700p

Art. 3 Oggetto e ambito di applicazione

Il presente regolamento disciplina le modalità di accesso e di uso delle risorse informatiche dell'Istituto dell'Istituzione scolastica (rete, apparecchiature e risorse infrastrutturali, patrimonio informativo e software).

Il presente Disciplinare si applica a tutti i dipendenti, senza distinzione di ruolo e/o livello, nonché a tutti i collaboratori dell'Azienda a prescindere dalla tipologia di rapporto contrattuale con la stessa intrattenuto (a titolo esemplificativo lavoratori somministrati, collaboratori a progetto, in stage, altro) oltre che ai dipendenti e collaboratori delle società esterne affidatarie di servizi, autorizzati ad accedere alla rete informatica dell'Azienda o che si trovino ad operare con dati o Strumenti dell'Azienda (tutti identificati nel presente documento col termine di "Utenti").

Gli eventuali controlli disposti in conformità e nel rispetto della vigente normativa escludono finalità di monitoraggio diretto ed intenzionale dell'attività lavorativa.

La progressiva diffusione delle nuove tecnologie informatiche ed in particolare l'accesso alla rete internet dal computer aziendale espone l'Azienda a possibili rischi di un coinvolgimento di rilevanza sia civile, sia penale, sia amministrativa, creando problemi alla sicurezza e all'immagine dell'Azienda stessa.

Art. 4 Diritti e Responsabilità

1. Ogni utente è responsabile civilmente e penalmente del corretto uso delle risorse informatiche, dei servizi/programmi ai quali ha accesso e dei propri dati. Tutti i soggetti interagenti col sistema informatico dell'Istituto sono anche responsabili di eventuali danni erariali conseguenti.

2. Tutti gli utenti che utilizzano internet devono rispettare:
   A. La legislazione vigente applicata alla comunicazione su internet
   B. La netiquette (etica e norme di buon uso dei servizi di rete)

Tutte le parti chiamate in causa dal presente documento devono leggerlo attentamente per accertarsi di averlo compreso in tutte le sue parti e di recepirne i contenuti.

3. La scuola propone di utilizzare internet al fine di promuovere l'eccellenza in ambito didattico, attraverso la condivisione delle risorse, l'innovazione e la comunicazione.

a) Il curricolo scolastico prevede che **gli studenti** imparino a reperire materiale, recuperare documenti e scambiare informazioni attraverso l'uso delle TIC. L'accesso ad internet diventa strumento di acquisizione del sapere che si affianca agli strumenti tradizionali e lo rende oggetto di particolare attenzione per la formazione dei giovani.
b) Per i **docenti**, la possibilità di accedere da scuola alle risorse documentarie tramite internet diviene un fattore imprescindibile per lo svolgimento della professione e per un uso corretto ed efficace delle nuove tecnologie per la didattica. Gli insegnanti hanno la responsabilità di guidare gli studenti nelle attività on line, di stabilire obiettivi chiari nell'uso di internet e di insegnarne un uso accettabile e responsabile.
c) Per il **personale ATA**, oltre alle attività legate alle proprie mansioni, l'utilizzo di internet è consentito e promosso per le attività legate all'aggiornamento e formazione del proprio profilo professionale autorizzate dal Dirigente o dal DSGA.

Via dei Platani, 5 - 21053 Castellanza
Tel. 0331/50.42.33 – Fax 0331/50.26.88
Email: vaic81700p@istruzione.it - vaic81700p@pec.istruzione
C.F. 81009410127 - CODICE MECCANOGRAFICO vaic 81700p

Art. 5 Utilizzo dei PC fissi e portatili di proprietà della scuola

1. Il personal computer affidato al dipendente è uno strumento di lavoro. Ogni utilizzo non inerente all'attività professionale può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza. Pertanto:

A. L'uso dell'elaboratore con profilo di accesso specifico (utenti con profilo Amministratore, Registro elettronico, piattaforma di e-Learning, account individuali riservati...) deve essere protetto da password; essa non deve essere divulgata.
B. Il personal computer deve essere **spento al termine dell'orario delle lezioni o di servizio**.
C. Al termine di qualunque sessione riservata di lavoro **è obbligatorio uscire dall'account**.
D. È vietato installare autonomamente programmi informatici sui server e sui Pc salvo autorizzazione esplicita del Dirigente Scolastico o del personale da esso indicato, in quanto sussiste il grave pericolo di portare virus informatici o di alterare la stabilità dell'elaboratore.
E. È vietato scaricare da internet software non autorizzati. In generale, i software utilizzabili sono solo quelli autorizzati dalla scuola.
F. È vietato modificare le caratteristiche impostate sul proprio Pc, salvo con autorizzazione esplicita del Dirigente Scolastico o del personale da esso indicato.
G. Non è consentito salvare file contenenti dati sensibili sui PC a cui possono accedere gli studenti.
H. Per utilizzare Pen Drive, CD ROM o altri supporti di memorizzazione personali è necessario sottoporli a controllo antivirus. Durante le attività, gli studenti non possono utilizzare file eseguibili (salvo gli applicativi di comune utilizzo) e utilità di sistema.

2. Il sistema informatico della scuola è provvisto di software antivirus aggiornato.La scuola pone in atto le misure preventive in suo possesso, ma ogni utente è informato che, considerata la vastità della problematica, esiste il pericolo reale di infettare il proprio supporto sul sistema della scuola, di conseguenza la scuola declina ogni responsabilità da ogni incidente che possa verificarsi da un eventuale infezione da virus.

Art. 6 Utilizzo della rete informatica

1. La rete didattica dell'istituto è fisicamente separata dalla rete amministrativa.
2. Le unità di rete sono aree di condivisione di informazioni strettamente professionali e non possono in alcun modo essere utilizzate per scopi diversi; pertanto qualunque file che non sia legato all'attività lavorativa non può essere dislocato in queste unità.
3. Il Dirigente Scolastico o il personale da esso indicato può in qualunque momento procedere alla rimozione di ogni file o applicazione che riterranno essere pericolosi per la sicurezza o in violazione del presente regolamento sia sui PC degli incaricati sia sulle unità di rete.
4. Le password d'ingresso alla rete ed ai programmi sono segrete e non vanno comunicate a terzi.

Nell'utilizzo della rete informatica è fatto divieto di:

A. Agire deliberatamente con attività che influenzino negativamente la regolare operatività della Rete e ne restringano l'utilizzabilità e le prestazioni per altri utenti.
B. Effettuare trasferimenti non autorizzati di informazioni (software, dati, ecc).
C. Installare componenti hardware non compatibili con l'attività istituzionale.
D. Rimuovere, danneggiare o asportare componenti hardware.
E. Utilizzare qualunque tipo di sistema informatico o elettronico per controllare le attività di altri utenti, per leggere, copiare o cancellare file e software di altri utenti.

Via dei Platani, 5 - 21053 Castellanza
Tel. 0331/50.42.33 – Fax 0331/50.26.88
Email: vaic81700p@istruzione.it - vaic81700p@pec.istruzione
C.F. 81009410127 - CODICE MECCANOGRAFICO vaic 81700p

F. Utilizzare software visualizzatori di pacchetti TCP/IP (sniffer), software di intercettazione di tastiera (keygrabber o keylogger), software di decodifica password (cracker) e più in generale software rivolti alla violazione della sicurezza del sistema e della privacy.
G. Usare l'anonimato o servirsi di risorse che consentano di restare anonimi.

Art. 7 Utilizzo di internet

1. La scuola non può farsi carico della responsabilità per il materiale trovato su internet o per eventuali conseguenze causate dalla navigazione.
2. Gli studenti imparano ad utilizzare i metodi di ricerca su internet, che includono l'uso dei motori di ricerca, e devono essere pienamente coscienti dei rischi a cui si espongono quando sono in rete. Devono essere educati a riconoscere e ad evitare gli aspetti negativi di internet come la pornografia, la violenza, il razzismo e lo sfruttamento dei minori. Agli studenti non deve essere sottoposto materiale di questo tipo e se ne venissero casualmente a contatto dovrebbero sempre riferire l'indirizzo internet (URL) ai responsabili.
3. L'utilizzo di internet comporta una serie di rischi che possono avere ripercussioni sulla gestione degli archivi sia di dati comuni sia sensibili:
   A. rischio interno relativo all'utilizzo della rete da parte di personale non autorizzato ad accedere ai dati;
   B. rischio esterno dovuto ad intrusioni nel sistema da parte di hacker/cracker;
   C. rischio interno dovuto ad intrusioni da parte di studenti;
   D. rischio interno/esterno di scaricamento di virus, Trojan e worm tramite posta elettronica e/o operazioni di download.

4. Nell'uso di internet **non sono consentite** le seguenti attività:
   A. l'uso di internet per motivi personali o che comunque esulano dall'attività lavorativa prevista dall'Istituto comprensivo e non espressamente autorizzati dal Dirigente;
   B. l'accesso a siti inappropriati (esempio siti pornografici, di intrattenimento, ecc.);
   C. lo scaricamento di software e di file non necessari all'attività istituzionale;
   D. utilizzare programmi per la condivisione e lo scambio di file in modalità peer to peer;
   E. accedere a flussi in streaming audio/video da Internet per scopi non istituzionali;
   F. un uso che possa in qualche modo recare qualsiasi danno all'Istituto o a terzi;
   G. accedere a social network o applicazione di instant messaging non autorizzati dal Dirigente;

5. La connessione wi-fi della scuola avviene tramite password, che può essere resa nota **s**olo al personale individuato dal Dirigente (docenti, personale tecnico-amministrativo e personale ATA).
6. Gli studenti non possono accedere ad internet se non sotto la supervisione di un docente.

Art. 8 Posta elettronica

L'utilizzo della posta elettronica istituzionale è connesso allo svolgimento dell'attività lavorativa. È fatto divieto di utilizzare le caselle di posta elettronica istituzionali per motivi diversi da quelli strettamente legati all'attività lavorativa. In questo senso, a titolo puramente esemplificativo, l'utente non potrà utilizzare la posta elettronica per:

- l'invio e/o il ricevimento di allegati contenenti fotografie, filmati o brani musicali (es. mp3) non legati all'attività lavorativa;

Via dei Platani, 5 - 21053 Castellanza
Tel. 0331/50.42.33 – Fax 0331/50.26.88
Email: vaic81700p@istruzione.it - vaic81700p@pec.istruzione
C.F. 81009410127 - CODICE MECCANOGRAFICO vaic 81700p

- l'invio e/o il ricevimento di messaggi personali o per la partecipazione a dibattiti, aste on line, concorsi, forum o mailing-list, catene telematiche, ecc. non legati all'attività lavorativa;
- l'invio di dati particolari (sensibili), es. dati sanitari.

La posta elettronica diretta all'esterno della rete informatica aziendale può essere intercettata da estranei e, conseguentemente, non deve essere utilizzata per inviare documenti o dati di lavoro contenenti dati personali.
In caso di necessità di trasmissione, per esigenze lavorative, di "dati personali" di terzi attraverso la posta elettronica tali dati devono essere cifrati e la chiave di decifrazione deve essere comunicata attraverso un altro canale.
La casella di posta deve essere mantenuta in ordine, cancellando documenti inutili e soprattutto allegati di dimensioni rilevanti.
Prima di aprire i file allegati ai messaggi di posta elettronica, è necessario identificare il mittente e porre particolare attenzione alla tipologia del file stesso, in caso in cui non si conosca il mittente è consigliabile procedere ad una verifica preventiva con il mittente (ad esempio tramite telefono) o eventualmente contattare il personale tecnico dell'Amministratore di sistema per una ulteriore verifica. Ciò al fine di evitare infezioni da virus, compromissione della propria PDL, perdita di dati personali, ecc.
Non si dovrà in alcun caso procedere all'apertura degli allegati a tali messaggi, questo per evitare l'infezione da virus informatici.
Al fine di garantire la funzionalità del servizio di posta elettronica aziendale e di ridurre al minimo l'accesso ai dati, nel rispetto del principio di necessità e di proporzionalità, il sistema, in caso di assenze programmate (ad es. per ferie o attività di lavoro fuori sede dell'assegnatario della casella) invierà automaticamente messaggi di risposta contenenti le "coordinate" di posta elettronica di un altro soggetto o altre utili modalità di contatto del Servizio di appartenenza. Tale funzionalità deve essere attivata dall'utente.

Gli Utenti, di norma, hanno in utilizzo indirizzi nominativi di posta elettronica strutturati con il format:
nome.cognome@istitutocomprensivocastellanza.edu.it

Per l'assolvimento di funzioni istituzionali, su richiesta degli uffici, vengono assegnate caselle e-mail con natura impersonale (con nomenclatura del tipo: info, amministrazione, fornitori, direttore, segreteria, ragioneria ecc.). Queste caselle di servizio saranno in ogni caso associate ad una o più persone fisiche responsabili del corretto utilizzo delle stesse. Il formato utilizzato sarà struttura@istitutocomprensivocastellanza.edu.it.
Un indirizzo e-mail può essere attribuito ad un gruppo di studenti o ad una classe nel caso di attività didattiche che prevedano scambio di informazioni con altri gruppi di studenti o classi nell'ambito di una precisa programmazione di una disciplina. Nell'uso di tale account, gli studenti devono attenersi al presente regolamento e riferire al docente o ai responsabili della didattica digitale se ricevono e-mail offensive; non devono rivelare dettagli o informazioni personali loro o di altre persone di loro conoscenza come indirizzi, numeri di telefono od organizzare incontri fuori dalla scuola.

Art. 9 Posta Elettronica in caso di assenze o cessazione

In caso di assenza improvvisa o prolungata e per improrogabili necessità legate all'attività lavorativa, qualora non sia possibile attivare la funzione autoreply o l'inoltro automatico su altre caselle istituzionali e si debba conoscere il contenuto dei messaggi di posta elettronica, il titolare della casella di posta può delegare, per il tempo strettamente necessario, un altro dipendente o l'Amministratore di Sistema per verificare il contenuto di messaggi e per inoltrare quelli ritenuti rilevanti per lo svolgimento dell'attività lavorativa.
Sarà compito del dipendente assicurarsi che sia redatto un verbale attestante quanto avvenuto e che sia informato il lavoratore interessato alla prima occasione utile.
In caso di interruzione del rapporto di lavoro con l'Utente, l'indirizzo di posta elettronica verrà disabilitato entro un periodo massimo di 30 giorni da quella data; entro 3 mesi, invece, si disporrà la definitiva e totale cancellazione dello stesso. In ogni caso, l'Istituto comprensivo si riserva il diritto di conservare i messaggi di posta elettronica che riterrà rilevanti.

Via dei Platani, 5 - 21053 Castellanza
Tel. 0331/50.42.33 – Fax 0331/50.26.88
Email: vaic81700p@istruzione.it - vaic81700p@pec.istruzione
C.F. 81009410127 - CODICE MECCANOGRAFICO vaic 81700p

Eventuali dati personali contenuti nei messaggi di posta elettronica vanno salvati dall'utente prima della cessazione del rapporto di lavoro.

Art. 10 Utilizzo delle password

1. Le password di ingresso alla rete, di accesso ai programmi e dello screensaver sono previste ed attribuite dai referenti di sistema.

2. Nel caso si sospetti che la password abbia perso la segretezza, deve essere immediatamente sostituita, dandone comunicazione scritta al Dirigente Scolastico.
3. Qualora l'utente venisse a conoscenza delle password di altro utente, è tenuto a darne immediata notizia, per iscritto, al Dirigente Scolastico.

Art. 10 Utilizzo dei supporti memorizzabili riutilizzabili

1. Tutti i supporti memorizzabili riutilizzabili (dischi, nastri, DAT, chiavi USB, CD e DVD) contenenti dati sensibili e giudiziari devono essere trattati con particolare cautela e ricorrendo a forme di criptazione e anonimizzazione dei dati onde evitare che il loro contenuto possa essere recuperato. I supporti magnetici contenenti dati sensibili e giudiziari (disciplinare tecnico Privacy) devono essere custoditi in archivi chiusi a chiave. Tutti i supporti magnetici riutilizzabili (dischetti, nastri, DAT, chiavi USB, CD riscrivibili e DVD) obsoleti devono essere consegnati al Dirigente Scolastico per l'opportuna distruzione.
2. Ogni qualvolta si procederà alla dismissione di un Personal Computer il Dirigente Scolastico o il personale da esso autorizzato provvederà alla distruzione o all'archiviazione protetta delle unità di memoria interne alla macchina stessa (hard-disk, memorie allo stato solido).
3. E' responsabilità dell'Utente salvare eventuali dati personali contenuti nel dispositivo prima della riconsegna dello stesso all'amministrazione. L'Istituto comprensivo non potrà essere ritenuto responsabile per la perdita di dati personali contenuti in strumenti dell'Istituto.

Art. 11 Utilizzo delle stampanti e dei materiali di consumo

1. L'utilizzo delle stampanti e dei materiali di consumo (carta, inchiostro, toner, supporti digitali come CD e DVD) è riservato esclusivamente ai compiti di natura strettamente istituzionale.

2. L'utilizzo delle strumentazioni e delle risorse messe a disposizione dall'amministrazione scolastica, inclusi telefoni, computer, stampanti, fotocopiatrici, materiale di cancelleria, pile, eccetera, è strettamente limitato alle attività lavorative e didattiche previste dall'istituto.

3. Qualsiasi uso personale o a vantaggio di soggetti individuali o giuridici esterni all'istituto è rigorosamente proibito. Questa politica mira a garantire la massima efficienza e correttezza nella gestione delle risorse pubbliche, salvaguardando l'integrità e il decoro dell'istituzione scolastica, nel prioritario rispetto della normativa vigente.

4. La violazione di queste disposizioni sarà considerata un uso improprio delle risorse dell'istituto e potrà comportare conseguenze previste dalle norme e dai regolamenti applicabili.
5. Devono essere evitati in ogni modo sprechi dei suddetti materiali o utilizzi eccessivi.
6. È cura dell'utente effettuare la stampa dei dati solo se strettamente necessaria e di ritirarla prontamente dai vassoi delle stampanti comuni.
7. E' proibito abbandonare documentazione digitale o a stampa.

Via dei Platani, 5 - 21053 Castellanza
Tel. 0331/50.42.33 – Fax 0331/50.26.88
Email: vaic81700p@istruzione.it - vaic81700p@pec.istruzione
C.F. 81009410127 - CODICE MECCANOGRAFICO vaic 81700p

8. Il telefono aziendale (fisso) assegnato all'utente è uno strumento di lavoro ne viene concesso l'uso esclusivamente per lo svolgimento dell'attività lavorativa, non sono quindi consentite comunicazioni a carattere personale o comunque non strettamente inerenti l'attività lavorativa stessa. L'effettuazione di telefonate personali non è consentita.
9. È vietato l'utilizzo dei fax istituzionali anche digitali per fini personali sia per spedire sia per ricevere documentazione.
10. Le stampanti di rete condivise sono installate per gruppi di lavoro, tramite policy di dominio.
11. Per quanto concerne l'uso delle stampanti gli utenti sono tenuti a:

- Effettuare la stampa dei dati solo se strettamente necessaria e di ritirarla prontamente dai vassoi.
- Prediligere le stampanti di rete condivise, rispetto a quelle locali/personali, per ridurre l'utilizzo di materiali di consumo (toner ed altri consumabili).
- Prediligere la stampa in bianco/nero e fronte/retro al fine di ridurre i costi, se possibile.
- Evitare di stampare documenti o file non adatti (molto lunghi o non supportati, come ad esempio il formato pdf o file di contenuto grafico) su stampanti di rete condivise.

12. Nel caso in cui si rendesse necessaria la stampa di dati personali, l'utente dovrà presidiare il dispositivo di stampa per evitare la possibile perdita o divulgazione di tali informazioni e persone terze non autorizzate.
13. Gli scanner di rete condivisi sono configurati per poter scansionare in cartelle di rete, legate ai gruppi di lavoro. Sarà cura dell'utente cancellare, dalla cartella condivisa, i documenti scansionati una volta verificata l'attività di scansione.
14. Le stampanti, le fotocopiatrici, gli scanner istituzionali devono essere spenti in caso di inutilizzo prolungato

Art. 12 Utilizzo di altre strumentazioni informatiche di proprietà della scuola

1. L'utilizzo di qualunque **hardware** di proprietà della scuola (LIM, proiettori, Smart TV ecc.) è responsabilità degli utenti. Non ne è consentito l'uso se non per scopi strettamente lavorativi.
3. Gli studenti e il personale esterno (tecnici informatici e consulenti) possono accedervi solo in presenza di un docente.
4. Gli utenti sono responsabili anche della manutenzione ordinaria (pulizia dei filtri e degli schermi, corretto stato dei cavi di alimentazione, conservazione di pennarelli, puntatori, telecomandi, ecc.).
Si ricorda che:

A. gli schermi possono e devono essere puliti solo con un panno asciutto;
B. la polvere è estremamente dannosa per le apparecchiature informatiche, e quindi si richiede e una particolare cura da parte degli utenti (non utilizzare il gesso vicino a PC e LIM, non appoggiare gli apparecchi a terra o in luoghi in cui si possano impolverare o bagnare).
C. Per preservare la durata delle lampade dei proiettori (anche delle LIM):
    a. non lasciare accesi gli schermi ed i proiettori per lungo tempo inutilizzati;
    b. non accendere e spegnere rapidamente i proiettori, ma attendere il necessario tempo di raffreddamento.
    c. spegnere il proiettore se dà messaggi riguardanti il surriscaldamento e la necessità di controllare il flusso d'aria; una volta completato il raffreddamento, controllare la pulizia del filtro;
    d. effettuare una pulizia periodica del filtro.

5. Tutte le apparecchiature informatiche devono essere spente alla fine delle lezioni o comunque alla fine delle attività didattiche.

6. I **software** distribuiti attraverso supporti memorizzabili fisici di proprietà della scuola devono essere conservati presso la Segreteria didattica; è compito dei docenti che li utilizzano assicurarsi che i supporti su cui sono conservati (CD, DVD, chiavi USB ecc.) e le password per l'installazione non vengano smarrite.

Art. 14 Divieti espressi

È espressamente vietato:

Via dei Platani, 5 - 21053 Castellanza
Tel. 0331/50.42.33 – Fax 0331/50.26.88
Email: vaic81700p@istruzione.it - vaic81700p@pec.istruzione
C.F. 81009410127 - CODICE MECCANOGRAFICO vaic 81700p

1. Comunicare le proprie informazioni personali o codici di accesso (nome utente e password) in risposta a richieste pervenute via e-mail (phishing).

2. Utilizzare l'indirizzo di posta elettronica contenente il dominio dell'Ente per iscriversi in qualsivoglia sito per motivi non attinenti all'attività lavorativa, senza espressa autorizzazione scritta dell'Azienda, nonché utilizzare il dominio dell'Istituto comprensivo per scopi personali.

3. Creare, archiviare o spedire, anche solo all'interno della rete aziendale, messaggi pubblicitari o promozionali o comunque allegati (filmati, immagini, musica o altro) non connessi con lo svolgimento della propria attività lavorativa, nonché partecipare a richieste, petizioni, mailing di massa di qualunque contenuto, "catene di Sant'Antonio" o in genere a pubblici dibattiti utilizzando l'indirizzo aziendale.

4. Trasmettere messaggi a tutti i dipendenti senza l'autorizzazione necessaria.

5. Sollecitare donazioni di beneficenza, propaganda elettorale o altre voci non legate al lavoro.

6. Simulare l'identità di un altro utente, ovvero utilizzare credenziali di posta, non proprie, per l'invio di messaggi.

7. Inviare, tramite la posta elettronica, anche all'interno della rete aziendale, materiale a contenuto violento, sessuale o comunque offensivo dei principi di dignità personale, di libertà religiosa, di libertà sessuale o di manifestazione del pensiero, anche politico.

Art. 10 Utilizzo di apparecchiature informatiche personali

1. Per quanto riguarda l'utilizzo di apparecchiature informatiche personali (PC portatili, smartphone, tablet) all'interno dei locali scolastici, tutti gli utenti sono tenuti a rispettare il presente regolamento, prestando particolare attenzione alla tutela della Privacy.
2. È fatto divieto agli studenti di utilizzare tali apparecchiature, salvo specifica autorizzazione degli insegnanti per motivazioni strettamente didattiche.
3. Ai dipendenti non è permesso connettere alla rete dell'Istituto comprensivo dispositivi personali.
4. Gli Utenti non dipendenti (ovvero i consulenti, collaboratori esterni e fornitori, ecc.), possono utilizzare i propri Strumenti personali per memorizzare dati e informazioni inerenti all'attività dell'Istituto comprensivo solo se espressamente autorizzati per iscritto dal Dirigente. In assenza di tale autorizzazione, l'utilizzo di strumenti personali deve considerarsi vietato.

Art. 11 Utilizzo di risorse informatiche in Cloud

1. Utilizzare un servizio di cloud computing per memorizzare dati personali o sensibili, espone l'Istituto comprensivo a potenziali problemi di violazione delle regole sulla riservatezza dei dati personali.
2. È vietato agli incaricati l'utilizzo di sistemi cloud (es. Dropbox, Google Drive, Apple iCloud, etc.) non espressamente approvati dall'Istituto comprensivo, in particolare è vietato condividere o registrare su sistemi cloud dati particolari ai sensi del Regolamento UE 679/2016 (GDPR).
3. L'Istituto comprensivo, tramite l'Amministratore di sistema, si riserva di identificare tecnologie e/o servizi cloud conformi alla normativa in materia di trattamento dei dati personali da mettere a disposizione degli Utenti.

Via dei Platani, 5 - 21053 Castellanza
Tel. 0331/50.42.33 – Fax 0331/50.26.88
Email: vaic81700p@istruzione.it - vaic81700p@pec.istruzione
C.F. 81009410127 - CODICE MECCANOGRAFICO vaic 81700p

Art. 13 Netiquette

E La netiquette è un insieme di regole, comunemente accettate e seguite da quanti utilizzano Internet e i servizi che la rete offre, che disciplinano il comportamento di un utente nel rapportarsi agli altri utenti attraverso risorse come wiki, newsgroup, mailing list, forum, blog o email.
Chiunque faccia utilizzo di comunicazioni digitali nell'espletamento delle attività lavorative previste dall'Istituto comprensivo deve rispettare le seguenti regole:
a) Rispettare le persone diverse per nazionalità, cultura, religione, sesso: il razzismo e ogni tipo di discriminazione sociale non sono ammessi;
b) Non essere intolleranti con chi ha scarsa dimestichezza con le TIC o commette errori concettuali;
c) Non rivelare dettagli o informazioni personali o di altre persone (indirizzi, numeri di telefono);
d) Richiedere sempre il permesso prima di iscriversi a qualche mailing-list o sito web che lo richieda;
e) Non dare indirizzo e numero di telefono a persone incontrate sul web, senza chiedere il permesso ai genitori o agli insegnanti (questo perché non si può avere la certezza dell'identità della persona con la quale si sta comunicando);
f) Non prendere appuntamenti con le persone conosciute tramite web senza aver interpellato prima gli insegnanti o i genitori; g) Non inviare fotografie proprie o di altre persone;
h) Riferire sempre a insegnanti e genitori se si incontrano in internet immagini o scritti che infastidiscono;
i) Se qualcuno non rispetta queste regole è opportuno parlane con gli insegnanti o con i genitori (alunni) o con il Dirigente scolastico (personale scolastico);
l) Chiedere il permesso prima di scaricare dal web materiale di vario tipo.

Art. 14 Osservanza delle disposizioni in materia di Privacy

È obbligatorio attenersi alle disposizioni in materia di Privacy del GDPR 679/2016 e alle misure minime di sicurezza previste, come indicate nella lettera di designazione di RESPONSABILE del trattamento dei dati.

Art. 15 Dirigente e Amministratori di Sistema

Solo il Dirigente Scolastico può fornire l'autorizzazione a personale interno o esterno per:

A. gestire l'hardware e il software di tutte le strutture tecniche informatiche di appartenenza dell'Istituto, collegate in rete o meno;
B. gestire esecutivamente (creazione, attivazione, disattivazione e tutte le relative attività amministrative) gli account di rete e i relativi privilegi di accesso alle risorse;
C. utilizzare le password oppure le credenziali di accesso di amministrazione del sistema;
D. solo se rientranti nelle normali attività di manutenzione, gestione della sicurezza e della protezione dei dati e nel pieno rispetto di quanto previsto riguardo ai diritti dei lavoratori, eseguire le seguenti attività:
   - Monitorare o utilizzare qualunque tipo di sistema informatico o elettronico per controllare il corretto utilizzo delle risorse di rete, dei computer e degli applicativi;
   - Creare, modificare, rimuovere o utilizzare qualunque account o privilegio;
   - Rimuovere programmi software dalle risorse informatiche assegnate agli utenti;
   - Rimuovere componenti hardware dalle risorse informatiche assegnate agli utenti.

Art. 16 Modalità di verifica

1. Le attività sull'uso del servizio di accesso a Internet e in generale dei servizi informatici sono automaticamente conservate in registri informatici (comunemente chiamati file di LOG) che riportano dettagli della navigazione, i siti e i documenti consultati e le operazioni verificatesi. I file di log contengono tipicamente:

- Data ed ora dell'operazione effettuata
- Utente che ha effettuato l'operazione
- Tipologia dell'operazione effettuata
- Dati associati all'operazione effettuata

Via dei Platani, 5 - 21053 Castellanza
Tel. 0331/50.42.33 – Fax 0331/50.26.88
Email: vaic81700p@istruzione.it - vaic81700p@pec.istruzione
C.F. 81009410127 - CODICE MECCANOGRAFICO vaic 81700p

2. In applicazione di quanto previsto dall'art. 5 del Regolamento Generale sulla Protezione Dei Dati (GDPR), l'Istituto comprensivo promuove ogni opportuna misura organizzativa e tecnologica volta a prevenire il rischio di utilizzi impropri e, comunque, a "minimizzare" l'uso di dati riferibili agli utenti e a tale scopo ha adottato ogni possibile strumento tecnico, organizzativo e fisico, volto a prevenire trattamenti illeciti sui dati trattati con strumenti informatici.
3. L'Istituto comprensivo informa di non adottare sistemi che determinano interferenza ingiustificata sui diritti e sulle libertà fondamentali di lavoratori, come pure di soggetti esterni che ricevono o inviano comunicazioni elettroniche di natura personale o privata.
4. In particolare, eventuali sistemi atti a monitorare eventuali violazioni di legge o comportamenti anomali da parte degli Utenti avvengono nel rispetto del principio di pertinenza e non eccedenza, con esclusione di registrazioni o verifiche con modalità sistematiche.
5. Qualora venga rilevato un non corretto utilizzo degli strumenti informatici messi a disposizione dall'Istituto comprensivo da parte dei singoli utenti, si procederà all'invio di un avviso all'utente, se minorenne, al titolare della responsabilità genitoriale. Sarà cura del responsabile interessato segnalare eventualmente l'evento al Dirigente per l'adozione degli atti di rispettiva competenza (es. procedimenti disciplinari).

Art. 16 Modalità di conservazione

I sistemi software sono stati programmati e configurati in modo da registrare nei log di sistema i dati relativi agli accessi a Internet, al traffico telematico ed alle operazioni effettuate sui sistemi informatici per un arco temporale non inferiore a 6 mesi, in funzione delle caratteristiche tecniche dell'apparato e/o dei sistemi disponibili.
Tali dati possono essere acceduti da figure tecniche istituzionalmente autorizzate ed in possesso delle opportune credenziali di accesso (a titolo esemplificativo: amministratori di sistema, tecnici di società esterne contrattualizzate per servizi di assistenza e manutenzione) e dall'Autorità giudiziaria in caso di presunti illeciti.
Un eventuale prolungamento dei tempi di conservazione viene valutato come eccezionale e deve aver luogo solo in relazione a:

- esigenze tecniche o di sicurezza, valutate dall' Amministratore di sistema e documentate in forma scritta
- indispensabilità del dato rispetto all'esercizio o alla difesa di un diritto in sede giudiziaria;
- obbligo di custodire o consegnare i dati per ottemperare ad una specifica richiesta dell'autorità giudiziaria o della polizia giudiziaria.

In questi casi, il trattamento dei dati personali è limitato alle sole informazioni indispensabili per perseguire finalità preventivamente determinate ed essere effettuato con logiche e forme strettamente correlate agli obblighi, compiti e finalità già esplicitati

Art. 17 Validità e pubblicazione

1. Il presente Disciplinare ha validità a decorrere dalla data della sua adozione.
2. Il disciplinare è oggetto di revisione a seguito di modifiche normative o in relazione ad eventuali evoluzioni tecniche in materia informatica e di telecomunicazioni.
3. Con l'entrata in vigore del presente Disciplinare tutte le disposizioni in precedenza adottate in materia, in qualsiasi forma comunicate, devono intendersi abrogate e sostituite dalle presenti.
4. Il presente Disciplinare verrà diffuso a tutti i dipendenti ai sensi dell'art. 7 della legge 300/70 e del CCNL di comparto tramite Registro elettronico (personale docente) e Segreteria digitale (personale ATA), nonché pubblicato nella sezione

Via dei Platani, 5 - 21053 Castellanza
Tel. 0331/50.42.33 – Fax 0331/50.26.88
Email: vaic81700p@istruzione.it - vaic81700p@pec.istruzione
C.F. 81009410127 - CODICE MECCANOGRAFICO vaic 81700p

"Le carte della scuola" del sito istituzionale raggiungibile all'indirizzo web https://istitutocomprensivocastellanza.edu.it/, all'Albo pretorio online e nella sezione Altri contenuti > Accessibilità e Catalogo dei dati, metadati e banche dati > Accessibilità e catalogo di dati, metadati e banche dati > Regolamenti di Amministrazione Trasparente.