



ISTITUTO COMPRENSIVO STATALE di CASIER

Scuola Primaria – Scuola Secondaria di 1° grado – Via Peschiere, 16 - 31030 DOSSON DI CASIER (TV)

Tel. 0422 380848/491560 - Cod. meccanografico: TVIC82300C

✉ mail: info@iccasier.gov.it - Pec: TVIC82300C@PEC.ISTRUZIONE.IT – Web: www.iccasier.gov.it

C/C/P 17097312 – Cod. Fisc. 80017580269 - IBAN: IT 79 J 01030 61960 000000649878



REGOLAMENTO SULL'USO DI STRUMENTAZIONI, DI INTERNET E DELLA POSTA ELETTRONICA

(POLICY DELLA SCUOLA)

Approvato con deliberazione del Consiglio di Istituto del [26 gennaio 2018](#).

Il presente regolamento entra in vigore il 27 gennaio 2018.

Viste la Legge 7 agosto 1990 n. 241 "Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi" e la Legge 11 febbraio 2005 "Modifiche ed integrazioni alla legge 7/8/90 n. 241 concernenti norme generali sull'azione amministrativa";

Visto il D. Lgs. n.242 del 19/03/96 "Modifiche ed integrazioni al decreto legislativo 19 settembre 1994, n. 626, recante attuazione di direttive comunitarie riguardanti il miglioramento della sicurezza e della salute dei lavoratori sul luogo di lavoro".

Visto il DPR del 28/12/2000 n. 445 "Testo Unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa"

Visto il D. Lgs. del 30/06/2003 n. 196 "Codice in materia di protezione dei dati personali" e sue ss.mm.ii.;

Visto il D.M. del 7 dicembre 2006, n. 305 "Regolamento recante identificazione dei dati sensibili e giudiziari"

Vista la deliberazione del CNIPA 19/12/2004 n. 11 "Regole tecniche dei documenti digitali";

Visto il D. Lgs. 7 marzo 2005 n. 82 "Codice dell'Amministrazione Digitale";

Visto il S.O. n. 93 aggiornato dal D. Lgs. 159 del 4/4/2006 recante "Disposizioni integrative e correttive al D.Lgs. 7/3/2005 n. 82;

Vista la legge 20 maggio 1970 n. 300 "Statuto dei Lavoratori";

Vista la Direttiva del Consiglio dei Ministri n. 2/2009 del 26/05/2009;

Ritenuto opportuno richiamare gli artt. 2086, 2087 e 2014 del Codice Civile;

Considerato che l'Istituto Comprensivo Statale di Casier tra i vari strumenti di lavoro ha messo a disposizione dei dipendenti accessi ad Internet e servizi di caselle di posta elettronica per lo svolgimento delle mansioni e compiti loro affidati;

Richiamato il principio generale che l'utilizzo delle risorse ICT che la scuola mette a disposizione dei dipendenti deve sempre ispirarsi a criteri di diligenza e correttezza normalmente adottati nell'ambito dei rapporti di lavoro;

Rilevato che l'Autorità Garante per la Privacy, con delibera n. 13 del 1.3.2007 (pubblicata in G.U. del 10.3.2007 n. 58) ha inteso precisare che è opportuno da parte dei Datori di Lavoro adottare un disciplinare interno redatto in modo chiaro, senza formule generiche ed adeguatamente pubblicizzato verso i singoli dipendenti interessati, anche ai fini dell'esercizio del potere disciplinare;

Ritenuto che l'adozione del regolamento consente di escludere l'applicabilità della normativa penale a tutela della corrispondenza elettronica poiché, essendo considerata strumento di lavoro, non può essere considerata corrispondenza privata;

Considerato, inoltre, che, se correttamente applicato e fatto rispettare, il regolamento può risultare un efficace strumento della Policy scolastica anche al fine di limitare il rischio di insorgenza di responsabilità amministrativa della Scuola;

Ritenuto, pertanto, di dover adottare apposito regolamento per l'utilizzo di Internet e della Posta Elettronica in cui è, tra l'altro, precisato che gli stessi sono strumenti aziendali e come tali soggetti anche a controlli secondo i principi ed i criteri di cui ai commi 5, 6 e 7 del citato Provvedimento del Garante e della normativa in tema di Protezione dei dati personali D. Lgs. 196/2003 n. 196 e del D.M. 35 del 7 dicembre 2006;

Tenuto conto che il regolamento si applica a tutti i dipendenti, senza distinzione di ruolo e/o livello, a tutti i collaboratori della scuola, interni od esterni, ai collaboratori a progetto ed a quelli

durante il periodo di stage, a prescindere dal rapporto contrattuale con la stessa intrattenuto, nonché agli alunni;

viene disposto il seguente

Disciplinare per l'utilizzo della strumentazione, della rete internet e della posta elettronica.

Sommario

Finalità	5
Ambito di applicazione	5
Principi generali	5
Valutazione del Rischio	5
Nomina dell'Amministratore di sistema e del Custode delle password	7
Assegnazione delle postazioni di lavoro	8
Utilizzo dei personal computer	8
Utilizzo di supporti magnetici	9
Utilizzo delle stampanti e dei materiali d'uso	9
Utilizzo di telefonini e altre apparecchiature	9
Utilizzo della rete informatica	10
Utilizzo delle password	10
Procedure di gestione delle credenziali di autenticazione	11
Utilizzo di internet	11
Utilizzo della posta elettronica	12
Gestione del sito Web della scuola	13
Gestione ed utilizzo del registro elettronico	13
Diritti e responsabilità dei dipendenti	13
Doveri di comportamento dei dipendenti	13
Controlli e sanzioni	14
Informativa agli utenti	14
Aggiornamento e revisione del Regolamento	14

Finalità

Il presente Regolamento disciplina le modalità di accesso e di uso delle strumentazioni, della Rete Informatica, telematica e dei servizi che, tramite la rete stessa, è possibile ricevere o offrire all'interno e all'esterno dell'Istituto per dare il supporto informativo documentario alla ricerca, alla didattica, all'aggiornamento e alle attività collaborative tra scuole ed enti, nonché per tutti gli adempimenti amministrativi di legge.

Ambito di applicazione

La rete dell'Istituto è costituita dall'insieme delle risorse informatiche, cioè:

-dalle componenti hardware/software e dagli apparati elettronici collegati alla rete informatica dell'Istituto,

-dall'insieme delle banche dati in formato digitale ed in generale di tutti i documenti prodotti tramite l'utilizzo dei suddetti apparati.

Il presente Regolamento si applica, senza distinzione di ruolo e/o livello, a tutti gli utenti interni (personale amministrativo, docenti e collaboratori scolastici) autorizzati ad accedere alla rete della scuola nell'ambito della propria attività lavorativa ordinaria e straordinaria e agli studenti nei limiti loro assegnati a scopi didattici ed educativi.

Analogamente il presente Regolamento si applica alla ditta che effettua attività di manutenzione e agli altri eventuali soggetti esterni autorizzati all'accesso a specifiche banche dati e a tutti i collaboratori dell'istituto a prescindere dal rapporto contrattuale con gli stessi intrattenuto (es. soggetti in attività di stage, relatori e formatori per corsi di aggiornamento, ...).

Principi generali

L'Istituto prevede l'utilizzo delle strumentazioni informatiche, della rete internet e della posta elettronica da parte degli utenti quali strumenti utili a perseguire le proprie finalità istituzionali e prevede che lo stesso si conformi ai seguenti principi:

-principio di necessità: i sistemi informativi e i programmi informatici vengono configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi in relazione alle finalità perseguite;

-principio di correttezza: le caratteristiche essenziali dei trattamenti sono rese note agli utenti;

-principio di pertinenza e non eccedenza: i trattamenti sono effettuati per finalità determinate, esplicite e legittime e i dati sono trattati nella misura meno invasiva possibile.

Valutazione del Rischio

La rete informatica di Istituto, l'accesso alla rete internet e alla posta elettronica, la strumentazione affidata al dipendente sono strumenti di lavoro; su di essi vengono effettuate regolari attività di controllo, amministrazione e back up ed essi non possono in alcun modo essere utilizzati per scopi diversi perché ogni utilizzo non inerente all'attività lavorativa può

contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza.

In relazione all'utilizzo non corretto di detti strumenti si individuano i seguenti possibili rischi e conseguenti effetti, rappresentati nella tabella sottostante:

Attività	Rischio	Motivazione	Possibile effetto
Manutenzione di periferiche hardware interne (scheda video, ecc.)	Alto	Possono essere danneggiati componenti interne e il PC	Danneggiamento della strumentazione
Manutenzione di periferiche hardware esterne (tastiera, mouse, ecc.)	Basso		Limitazione nell'utilizzo
Download non controllato o non programmato di aggiornamenti relativi ad applicazioni installate dal responsabile di rete	Alto	Possono essere scaricate applicazioni non verificate con il pericolo di portare Virus informatici o di alterare la stabilità delle applicazioni dell'elaboratore	Danneggiamento del software del PC o della rete informatica interna
Download controllato o programmato di aggiornamenti relativi ad applicazioni installate dal responsabile di rete	Basso		
Download di dati non inerenti alle attività lavorative (musica, giochi, ecc.)	Alto	Possono essere scaricate applicazioni non verificate con il pericolo di portare virus informatici o di alterare la stabilità delle applicazioni dell'elaboratore	Danneggiamento del software del PC o della rete informatica interna. Gravi responsabilità civili e penali per l'Istituto in caso di violazione della normativa a tutela dei diritti d'autore.
Installazione di applicazioni senza l'autorizzazione del responsabile della rete	Alto	Possono essere installate applicazioni non compatibili	Danneggiamento del software del PC o della rete informatica interna

Accesso alla rete effettuato da Pc di proprietà dell'utente	Alto	Accessi non autorizzati alla rete	Furto di dati
Apertura di allegati di posta elettronica di incerta provenienza	Alto	Possono contenere Malware/Spyware	Danneggiamento del software del PC o della rete informatica interna. Divulgazione di password e dati riservati
Elaboratore connesso alla rete lasciato incustodito o divulgazione di password	Alto	Possibile utilizzo da parte di terzi	Uso indebito di dati riservati, danneggiamento della rete informatica interna
Utilizzo di supporti removibili esterni non autorizzati	Alto	Possono essere trasferite applicazioni dannose per il PC nella rete informatica	Danneggiamento dei PC o della rete informatica interna
Furto di dati Mancata distruzione o perdita accidentale di supporti magnetici riutilizzabili (dischetti, nastri, DAT, chiavi usb, cd riscrivibili , ...) contenenti dati sensibili e giudiziari	Alto	Recupero di dati memorizzati anche dopo la loro cancellazione	Uso indebito di dati riservati

Nomina dell'Amministratore di sistema e del Custode delle password

Il datore di lavoro conferisce all'Amministratore di sistema il compito di sovrintendere alle risorse informatiche dell'Istituto assegnandogli in maniera esclusiva le seguenti attività:

- a) gestione dell'hardware e del software (installazione, aggiornamento, rimozione) di tutte le strutture tecniche informatiche dell'istituto, siano esse collegate in rete o meno;
- b) configurazione dei servizi di accesso alla rete interna, ad internet e a quelli di posta elettronica con creazione, attivazione e disattivazione dei relativi account;
- c) attivazione della password di accensione (BIOS);
- d) creazione di un'area condivisa sul server per lo scambio di dati tra i vari utenti, evitando condivisioni dei dischi o di altri supporti configurati nel PC che non siano strettamente necessarie perché sono un ottimo "aiuto" per i software che cercano di "minare" la sicurezza dell'intero sistema;

e) controllo del corretto utilizzo delle risorse di rete, dei computer e degli applicativi, durante le normali attività di manutenzione, gestione della sicurezza e della protezione dei dati e nel pieno rispetto di quanto previsto riguardo ai diritti dei lavoratori;

f) rimozione sia sui PC degli incaricati sia sulle unità di rete, di ogni tipo di file o applicazione che può essere pericoloso per la sicurezza o costituisce violazione del presente regolamento;

g) distruzione delle unità di memoria interne alla macchina (hard - disk, memorie allo stato solido) ogni qualvolta si procederà alla dismissione di un PC e dei supporti removibili consegnati a tale scopo dagli utenti;

h) utilizzo delle credenziali di amministrazione del sistema per accedere ai dati o alle applicazioni presenti su una risorsa informatica assegnata ad un utente in caso di indispensabile ed indifferibile necessità di intervento per prolungata assenza, irrintracciabilità o impedimento dello stesso, solo per il tempo necessario al compimento di attività indifferibili e solo su richiesta del Responsabile del trattamento.

L'Amministratore di sistema, nell'espletamento delle sue funzioni legate alla sicurezza e alla manutenzione informatica, ha facoltà di accedere in qualunque momento, anche da remoto, e dopo aver richiesto l'autorizzazione all'utente interessato, al PC di ciascun utente.

Il Custode delle password è incaricato di custodire e conservare in luogo riservato e sicuro, in formato cartaceo, le credenziali. E' tenuto a ottemperare al suo compito avendo cura di non diffondere, nemmeno accidentalmente, le stesse a persone estranee al loro utilizzo.

Assegnazione delle postazioni di lavoro

Per ridurre il rischio di impieghi abusivi o dannosi, il datore di lavoro provvede a:

-individuare preventivamente le postazioni di lavoro e assegnarle a ciascun dipendente,
-individuare preventivamente gli utenti a cui è accordato l'utilizzo della posta elettronica e l'accesso a internet.

La strumentazione dell'Istituto non è di esclusivo dominio del dipendente, ma rientra tra i beni a cui determinati soggetti possono comunque sempre accedere. L'eventuale accesso del datore di lavoro, qualora necessiti di informazioni contenute nei documenti residenti sul PC assegnato al dipendente, è legittimo.

Utilizzo dei personal computer

Gli utenti utilizzano per il proprio lavoro soltanto computer di proprietà dell'Istituto di cui sono responsabili, salvo eccezioni autorizzate dal datore di lavoro e dall'Amministratore di sistema.

Sono tenuti a:

- applicare al PC portatile le regole di utilizzo previste per i PC connessi in rete,
- custodirlo con diligenza e in luogo protetto durante gli spostamenti,
- rimuovere gli eventuali file elaborati sullo stesso prima della sua riconsegna,
- non disattivare sul PC lo screen saver e la relativa password,
- conservare la password nella massima riservatezza e con la massima diligenza,
- non modificare la configurazione hardware e software del PC se non esplicitamente autorizzati dall'amministratore di sistema,
- non rimuovere, danneggiare o asportare componenti hardware,
- nel caso il software antivirus rilevi la presenza di un virus, sospendere immediatamente ogni elaborazione in corso, senza spegnere il PC e segnalare prontamente l'accaduto al personale incaricato dell'assistenza tecnica,
- permettere l'autoaggiornamento del PC,

- prestare la massima attenzione ai supporti di origine esterna (es. pendrive), verificando preventivamente, tramite il programma antivirus, ogni file acquisito attraverso qualsiasi supporto e avvertendo immediatamente l'Amministratore di sistema nel caso in cui vengano rilevati virus o eventuali malfunzionamenti,
- non lasciare incustodita e accessibile la propria postazione una volta eseguita la connessione al sistema con le proprie credenziali di autenticazione,
- non cedere, una volta superata la fase di autenticazione, l'uso della propria stazione a persone non autorizzate, in particolar modo per quanto riguarda l'accesso ad internet e ai servizi di posta elettronica,
- spegnere il PC al termine del lavoro o in caso di assenze prolungate dalla propria postazione.

Utilizzo di supporti magnetici

Gli utenti devono trattare con particolare cura i supporti magnetici (dischetti, nastri, DAT, chiavi USB, CD riscrivibili,...) in particolar modo quelli riutilizzabili, per evitare che persone non autorizzate possano accedere ai dati ivi contenuti. Di conseguenza le azioni da compiere obbligatoriamente sono le seguenti:

- a) porre attenzione nell'utilizzo dei supporti rimovibili personali,
- b) custodire i supporti magnetici contenenti dati sensibili e giudiziari in armadi chiusi a chiave onde evitare che il loro contenuto possa essere trafugato o alterato e/o distrutto (presso il custode delle password),
- c) consegnare i supporti magnetici riutilizzabili (dischetti, nastri, DAT, chiavi USB, CD riscrivibili, ...) obsoleti all'Amministratore di sistema per l'opportuna distruzione onde evitare che il loro contenuto possa essere successivamente alla cancellazione recuperato.

Utilizzo delle stampanti e dei materiali d'uso

Stampanti e materiali di consumo in genere (carta, inchiostro, toner, supporti digitali come CD e DVD) 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, distruggere personalmente e sistematicamente le stampe che non servono più.

Utilizzo di telefonini e altre apparecchiature

Il telefono affidato al dipendente è uno strumento di lavoro. Ne viene concesso l'uso esclusivamente per lo svolgimento delle attività lavorative, non essendo quindi consentite comunicazioni a carattere personale o comunque non strettamente inerenti all'attività lavorativa stessa.

La ricezione o l'effettuazione di telefonate personali sono consentite solo nel caso di comprovata necessità ed urgenza, mediante il telefono fisso a disposizione.

Al cellulare d'Istituto qualora venisse assegnato, si applicano le medesime regole sopra previste.

È vietato l'utilizzo del fax e delle fotocopiatrici d'Istituto per fini personali.

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

- a) diversa disposizione esplicita del titolare del trattamento, da concordarsi di volta in volta e comunque sempre preventivamente al trattamento,
- b) informazione preventiva degli interessati,
- c) acquisizione del loro libero consenso, preventivo ed informato.

Utilizzo della rete informatica

Le reti interne, presenti in ciascuno dei tre plessi (di scuola secondaria di primo grado e di scuola primaria), collegano tutti i computer presenti in ogni singolo edificio. L'accesso ad internet è gestito da quattro connessioni distinte: tre connessioni WDSL (CloudItalia), riservate alla segreteria, alle aule della scuola secondaria di primo grado (in via Peschiere, 16) e della scuola primaria (in via Fermi, 11) situate a Dosson di Casier e una connessione ADSL (Eolo) per la navigazione delle aule della scuola primaria di Casier (in via Basse, 1).

La rete informatica permette di salvare su server i files relativi alla produttività individuale. Le cartelle presenti nei server di segreteria e di laboratorio sono aree di condivisione di informazioni strettamente professionali e non possono in alcun modo essere utilizzate per scopi diversi. Su queste unità vengono svolte regolari attività di controllo, amministrazione e back-up.

L'accesso è regolamentato da policies di sicurezza che suddividono gli accessi fra gruppi e utenti.

Periodicamente si provvede alla pulizia degli archivi, con cancellazione dei files obsoleti ed inutili.

Gli utenti della rete informatica sono tenuti a utilizzare la rete in modo conforme a quanto stabilito dal presente regolamento e quindi:

- a) mantenere segrete e non comunicare a terzi, inclusi gli amministratori di sistema, le password d'ingresso alla rete ed ai programmi e non permettere ad alcuno di utilizzare il proprio accesso,
- b) provvedere periodicamente alla pulizia degli archivi con cancellazione dei file obsoleti o inutili ed evitare un'archiviazione ridondante,
- c) verificare preventivamente ogni archivio elettronico (file) acquisito attraverso qualsiasi supporto (es. pendrive) prima di trasferirlo su aree comuni della rete.

Agli utenti è fatto espresso divieto di influenzare negativamente la regolare operatività della rete, interferendo con la connettività altrui o con il funzionamento del sistema e quindi di:

- a) utilizzare qualunque tipo di sistema informatico o elettronico per controllare le attività di altri utenti, per leggere, copiare o cancellare files o software di altri utenti, 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 delle privacy,
- b) sostituirsi a qualcuno nell'uso dei sistemi, cercare di catturare password altrui o forzare password o comunicazioni criptate,
- c) modificare le configurazioni impostate dall'amministratore di sistema,
- d) limitare o negare l'accesso al sistema a utenti legittimi,
- e) effettuare trasferimenti non autorizzati di informazioni (software, dati, ...),
- f) distruggere o alterare dati altrui,
- g) usare l'anonimato o servirsi di risorse che consentano di restare anonimi.

Utilizzo delle password

Per l'accesso alla strumentazione informatica di Istituto ciascun utente deve essere in possesso delle specifiche credenziali di autenticazione previste ed attribuite dall'incaricato della custodia delle password.

Le credenziali di autenticazione per l'accesso alla rete consistono in un codice per l'identificazione dell'utente (user id) associato ad una parola chiave (password) riservata che dovrà essere custodita dal Custode delle password con la massima diligenza e non può essere divulgata.

Procedure di gestione delle credenziali di autenticazione

È necessario procedere alla modifica della parola chiave, a cura dell'incaricato, al primo utilizzo. Se l'utente non provvede autonomamente a variare la password entro i termini massimi, viene automaticamente disabilitato. Provvederà l'Amministratore di sistema a riabilitare l'utente e ad assegnargli una password provvisoria che l'utente dovrà cambiare al primo accesso.

Per scegliere una parola chiave si devono seguire le seguenti istruzioni:

- usare una parola chiave di almeno otto caratteri,
- usare una combinazione di caratteri alfabetici e numerici (meglio inserire anche segni di interpunzione o un carattere speciale),
- non usare mai il proprio nome o cognome, né quello di congiunti (le migliori password sono quelle facili da ricordare, ma allo stesso tempo difficili da indovinare, come quelle che si possono ottenere comprimendo frasi lunghe).

La password deve essere cambiata a intervalli regolari a cura dell'incaricato del trattamento d'intesa con il custode della password (ogni sei mesi) e comunicata al custode delle password perché ne curi la conservazione.

Bisogna evitare di comunicarla ad altri, di trascriverla su supporti (agenda, post-it, ...) che siano accessibili ad altri o di consentire che qualcuno sbirci quello che si sta scrivendo sulla tastiera quando viene immessa la password.

Nel caso si sospetti che la password abbia perso la segretezza essa deve essere immediatamente sostituita.

Utilizzo di internet

La navigazione in internet costituisce uno strumento necessario allo svolgimento della propria attività lavorativa. L'accesso ad internet è regolato da filtri predefiniti dall'amministratore di sistema su autorizzazione dell'amministrazione, con esclusione dei siti istituzionali.

Il titolare del trattamento provvede alla individuazione delle categorie di siti considerati correlati o non correlati con la prestazione lavorativa.

L'Amministratore di sistema provvede alla configurazione di sistemi e all'utilizzo di filtri che prevengono determinate operazioni non correlate all'attività lavorativa (es. upload, restrizione nella navigazione, download di file o software).

L'accesso alla navigazione in internet deve essere effettuato esclusivamente a mezzo della rete di istituto e solo per fini lavorativi o di studio. L'utilizzo responsabile di modem personali è sconsigliato e comunque deve essere autorizzato dall'Amministratore di sistema.

Gli utenti sono tenuti ad utilizzare l'accesso ad internet in modo conforme a quanto stabilito dal presente regolamento e quindi devono navigare solamente in siti attinenti allo svolgimento delle mansioni assegnate.

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

- a) fare conoscere ad altri la password del proprio accesso,
 - b) usare internet per motivi personali,
 - c) servirsi dell'accesso internet per attività in violazione del diritto d'autore o di altri diritti tutelati dalla normativa vigente,
 - d) accedere a siti pornografici, di intrattenimento, ...,
 - e) scaricare i software gratuiti dalla rete, salvo casi di comprovata utilità e previa autorizzazione in tal senso da parte del responsabile,
 - f) utilizzare programmi per la condivisione e lo scambio di file in modalità peer to peer (Napster, Emule, Winmx, e-Donkey,...)
 - g) ascoltare la radio o guardare video o filmati utilizzando le risorse internet, se non attinenti l'attività lavorativa o direttamente autorizzati dal responsabile del trattamento,
 - h) effettuare transazioni finanziarie, operazioni di remote banking, acquisti on-line e simili, se non attinenti l'attività lavorativa o direttamente autorizzati dal Responsabile del trattamento,
 - i) inviare fotografie, dati personali o di amici dalle postazioni internet.
- Al termine dell'utilizzo della rete è obbligatorio effettuare il logout.

Utilizzo della posta elettronica

L'istituto mette a disposizione dei lavoratori indirizzi di posta elettronica individuali in dominio istituzionale @iccasier.it (servizio di posta interno all'Istituto) che consentono:

- di inviare e ricevere comunicazioni attinenti allo svolgimento dell'attività lavorativa,
- di partecipare a gruppi di lavoro in condivisione e collaborazione, attinenti allo svolgimento dell'attività lavorativa.

Tramite la posta istituzionale con dominio @iccasier.it possono essere trasmesse le seguenti comunicazioni:

- convocazioni riunioni;
- comunicazioni di servizio anche dirette al singolo dipendente;
- materiale preparatorio alle riunioni collegiali;
- circolari;
- copia elettronica di documenti redatti su supporti cartacei (purché in formati e dimensioni opportune).

Ogni utente assegnatario di una casella di posta elettronica istituzionale è responsabile del corretto utilizzo della stessa ed è tenuto a utilizzarla in modo conforme a quanto stabilito dal presente regolamento, quindi deve:

- a) conservare la password nella massima riservatezza e con la massima diligenza,
- b) mantenere la casella in ordine, cancellando documenti inutili e allegati ingombranti,
- c) utilizzare l'account per l'invio di comunicazioni attinenti all'attività lavorativa,
- d) inviare preferibilmente file in formato PDF,
- e) al termine delle operazioni effettuare il logout dall'account.

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

- a) prendere visione della posta altrui,
- b) simulare l'identità di un altro utente, ovvero utilizzare per l'invio di messaggi credenziali di posta non proprie, nemmeno se fornite volontariamente o di cui si ha casualmente conoscenza,
- c) utilizzare strumenti software o hardware atti ad intercettare il contenuto delle comunicazioni informatiche all'interno dell'istituto,
- d) 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,
- e) utilizzare il servizio di posta elettronica per inoltrare giochi, scherzi, barzellette, appelli e petizioni, messaggi tipo "catene" e altre e-mails che non siano di lavoro.

Gestione del sito Web della scuola

L'Istituzione Scolastica possiede un Sito Web per la gestione del quale è stato nominato un referente.

In nessun caso l'Istituto Comprensivo potrà essere ritenuto responsabile dei danni di qualsiasi natura causati direttamente o indirettamente dall'accesso al sito, dall'incapacità o impossibilità di accedervi, dall'affidamento dell'utente e dall'utilizzo dei contenuti.

L'Istituto provvederà ad inserire nel sito informazioni e comunicazioni aggiornate, rubriche, notizie, eventi, articoli relativi alle attività didattiche dell'Istituto.

I documenti sono pubblicati in formato .pdf.

Le informazioni relative alle persone da contattare includono solo l'indirizzo (posta elettronica e numero telefonico) della scuola e non dati personali.

Gestione ed utilizzo del registro elettronico

L'Istituzione Scolastica possiede un registro elettronico gestito da un Amministratore.

Tutti i dati relativi agli utenti che utilizzano il software sono protetti da password e sarà compito di ogni utente conservare e custodire le proprie credenziali.

Diritti e responsabilità dei dipendenti

Per assicurare la tutela dei diritti, delle libertà fondamentali e della dignità dei lavoratori, garantendo che sia assicurata una ragionevole protezione delle loro sfera di riservatezza nelle relazioni personali professionali, il trattamento dei dati mediante l'uso delle tecnologie telematiche è conformato al rispetto dei diritti delle libertà fondamentali nonché della dignità dell'interessato, dei divieti posti dallo statuto dei lavoratori sul controllo a distanza e dei principi di necessità, correttezza e finalità determinate, esplicite e legittime.

Ogni utente è responsabile, sia sotto il profilo civile che penale, del corretto uso delle risorse informatiche, dei servizi e dei programmi ai quali ha accesso e dei dati che tratta.

Spetta ai docenti vigilare affinché gli studenti loro affidati rispettino il regolamento e sono ne direttamente responsabili.

Doveri di comportamento dei dipendenti

Le strumentazioni informatiche, la rete internet e la posta elettronica devono essere utilizzate dal personale e dagli studenti sotto il controllo dei loro docenti, come strumenti di lavoro e studio.

Ogni loro utilizzo non inerente l'attività lavorativa e di studio è vietato in quanto può comportare disservizi, costi di manutenzione e soprattutto minacce alla sicurezza.

In particolare non può essere dislocato nelle aree di condivisione della rete alcun file che non sia legato all'attività lavorativa, nemmeno per brevi periodi.

Agli utenti è severamente vietata la memorizzazione di documenti informatici di natura oltraggiosa o discriminatoria per sesso, lingua, religione, razza, origine etnica, condizioni di salute, opinioni, appartenenza sindacale politica.

Non è consentito scaricare, scambiare o utilizzare materiale coperto dal diritto d'autore.

Controlli e sanzioni

Il datore di lavoro, per esigenze organizzative, per garantire la sicurezza sul lavoro, per evitare reiterati comportamenti dolosi illeciti può avvalersi legittimamente, nel rispetto dell'art. 4 comma 2 dello statuto dei lavoratori, di sistemi che consentano un controllo a distanza e determinato di dati personali riferibili a singoli utenti.

La lettura e la registrazione sistematica del servizio di accesso ad internet vengono automaticamente registrate.

Tali file possono essere messi a disposizione dell'autorità giudiziaria in caso di accertata violazione della normativa vigente.

Le registrazioni possono essere utilizzate per fornire informazioni esclusivamente su:

-numero di siti visitati da ciascun utente, quantità totale di dati scaricati, postazioni di lavoro utilizzate per la navigazione.

Qualora i controlli evidenzino un utilizzo anomalo degli strumenti informatici dell'istituto, il titolare del trattamento 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, ...) 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 nelle forme e con le modalità previste dall'istituto per gli studenti (vedere Regolamento di Istituto e di disciplina), dai contratti di lavoro per i dipendenti e attraverso l'adozione degli atti di specifica competenza nel caso di personale non dipendente,

-può portare alle azioni civili e penali consentite.

L'utilizzo dei servizi di accesso ad internet cessa o viene sospeso d'ufficio quando:

-non sussiste più la condizione di dipendente/studente o l'autorizzazione al loro uso,

-vi è il sospetto di manomissione dell'hardware o del software,

-in caso di diffusione o comunicazione a terzi da parte del dipendente di password, codici di accesso ecc. ...,

-in caso di accesso doloso a file o servizi non rientranti tra quelli autorizzati,

-ogni qualvolta sussistano ragionevoli evidenze di una violazione degli obblighi dell'utente che mette a rischio il sistema.

Informativa agli utenti

Il presente regolamento è messo a disposizione degli utenti, per la consultazione, sui mezzi di comunicazione interna utilizzati dall'istituto (circolare, sito) e quindi portato a conoscenza di ciascun dipendente.

L'utente qualora l'istituto decidesse di perseguire, per fini legati alla sicurezza dell'intero sistema informativo, il controllo della posta elettronica e della navigazione in internet, viene informato degli strumenti e dei modi di trattamento effettuati prime che questo sia iniziato.

Aggiornamento e revisione del Regolamento

Il presente regolamento è soggetto a revisione con frequenza annuale e ogni qualvolta sia necessario un aggiornamento alla luce dell'esperienza, di nuove normative e dell'innovazione tecnologica.

Tutti gli utenti possono proporre quando ritenuto necessario, integrazioni al presente regolamento e le proposte saranno esaminate dal Responsabile del trattamento in collaborazione con l'Amministratore di sistema.

Il Dirigente Scolastico
Elisabetta Costa-Reghini