Repubblica Italiana

Provincia Autonoma di Trento

ISTITUTO COMPRENSIVO "BERNARDO CLESIO" CLES

Via E. Chini 31 – 38023 Cles (Trento) – C.F. 92013820227
Tel 0463 421457 Fax 0463 424830
Mailto: segr.ic.cles@scuole.provincia.tn.it www.iccles.it

disciplinare per l'utilizzo degli strumenti elettronici

PRIVACY & SICUREZZA DELLE INFORMAZIONI DISCIPLINARE INTERNO SULL'UTILIZZO DELLE RISORSE INFORMATICHE

1. INTRODUZIONE

La nostra organizzazione mette a **disposizione degli addetti:**

- strumenti di informatica individuale, quali Personal Computer (PC) installati sul posto di lavoro, computer portatili ecc.
- servizi di posta elettronica ed internet.

Tali risorse costituiscono un mezzo di lavoro e devono essere utilizzati, di norma, per il perseguimento di fini strettamente connessi agli incarichi lavorativi secondo criteri di massima correttezza e professionalità, coerentemente al tipo di attività svolta ed in linea con le disposizioni normative vigenti.
Il documento illustra le norme generali di utilizzo di tali risorse che il personale e i collaboratori devono rispettare al fine di mitigare i rischi che un uso improprio degli stessi può determinare alla sicurezza del patrimonio informativo.
In particolare, l'utilizzo delle risorse informatiche non inerenti all'attività lavorativa può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza delle infrastrutture della nostra organizzazione.
Nella definizione delle norme comportamentali da osservare si è tenuto conto di quanto previsto dalla normativa vigente in materia e, in particolare, dal Decreto Legislativo 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali" e dai provvedimenti emessi dall'Autorità Garante per la protezione dei dati personali. Tra questi rientrano le "Linee guida del Garante per posta elettronica e internet" emesse in data 1 marzo 2007.
Va, infine, evidenziato che il titolare del trattamento dati della nostra organizzazione si riserva di verificare, nei limiti consentiti dalle norme legali e contrattuali e con modalità diffuse ed uniformi, il rispetto delle presenti istruzioni e l'integrità dei propri sistemi.

2. CESSAZIONE DEL RAPPORTO DI LAVORO

In caso di cessazione del rapporto di lavoro, l'utente deve mettere a disposizione del nostro responsabile trattamento dati qualsiasi risorsa assegnata, sia le attrezzature informatiche sia le informazioni di interesse aziendale:

- la casella di posta elettronica individuale sarà mantenuta attiva per il tempo strettamente necessario a gestire il passaggio di consegne e concludere eventuali contatti aperti;

- l'utente non può cancellare le informazioni di interesse aziendale presenti sulle postazioni di lavoro e/o sulla rete, senza esplicita autorizzazione del responsabile trattamento dati;
- qualora l'utente abbia inavvertitamente lasciato sulle postazioni di lavoro e/o sulla rete informazioni di interesse non aziendale, le stesse verranno cancellate senza alcuna responsabilità per la nostra organizzazione.

3. SANZIONI DISCIPLINARI

L'inosservanza delle norme comportamentali, descritte nel presente documento, può comportare l'applicazione delle sanzioni disciplinari previste dalle vigenti disposizioni del codice di disciplina applicabili ovvero di altre misure di tutela del caso.

Utilizzo delle postazioni di lavoro

La nostra organizzazione ha disposto che, in funzione del ruolo e delle esigenze lavorative, il personale in servizio venga dotato di personal computer (PC) per lo svolgimento di attività strettamente connesse agli incarichi lavorativi e comunque nel rispetto delle regole di seguito descritte. Le postazioni di lavoro, di regola, sono connesse alla rete interna della nostra organizzazione, con lo scopo di condividere informazioni, usufruire di servizi ed, in particolare, accedere alle applicazioni software necessarie alla gestione dei lavori.

Per una corretta gestione della postazione di lavoro è necessario che vengano osservate le seguenti regole:

- non è consentito aprire e manomettere le attrezzature informatiche messe a disposizione;
- non è consentito modificare le configurazioni software ed hardware impostate sulla propria postazione di lavoro, salvo previa autorizzazione dell'amministratore di sistema;
- la postazione di lavoro e le relative periferiche, quali stampanti locali e di rete, scanner, ecc.., devono essere spente al termine dell'attività lavorativa o in caso di assenze prolungate dall'ufficio. Eventuali eccezioni dovranno essere formalmente autorizzate dall'amministratore di sistema;
- non è consentita l'installazione di programmi software diversi da quelli predisposti;
- non è consentita la disinstallazione dei programmi software standard adottati;
- non è consentita la riproduzione o la duplicazione di programmi software nel rispetto della normativa vigente in materia di diritto di proprietà intellettuale;
- non utilizzare dischetti, CD-Rom o altri supporti di archiviazione removibili di provenienza incerta e tali da poter creare un danno alla postazione di lavoro
- non è consentito spostare le attrezzature informatiche senza la preventiva autorizzazione;
- non è consentita l'installazione non autorizzata di dispositivi di connessione propri;
- proteggere, in caso di abbandono momentaneo, la postazione richiamando le funzioni di sicurezza del sistema operativo ed assicurandosi della attivazione della funzione Lock Workstation o, in alternativa, impostando lo screen saver con password in modo che si attivi dopo 10/15 minuti di inattività o chiudere la sessione di lavoro. Lasciare la postazione incustodita e connessa alla rete può essere causa di utilizzo da parte di terzi non autorizzati senza che vi sia la possibilità di provarne l'indebito uso;

L'utente è responsabile delle attrezzature che gli sono affidate in uso e, pertanto, deve provvedere a mantenerle in completa efficienza segnalando tempestivamente ogni eventuale problema tecnico e, in caso di dubbio, sulla sicurezza della postazione di lavoro.

Gestione della password

Per una corretta gestione delle password, è necessario che vengano osservate le seguenti regole:

- modificare, alla prima connessione, la password che l'amministratore di sistema ha attribuito di default;

- cambiare la password obbligatoriamente ogni 6 mesi e, nel caso di trattamento di dati sensibili e/o giudiziari, ogni 90 giorni o immediatamente nei casi in cui sia compromessa;
- comporre la password con almeno 8 caratteri alfanumerici, o nel caso in cui lo strumento elettronico non lo consenta, con un numero di caratteri pari al massimo consentito e usare;
- preferibilmente, nella composizione della password almeno un carattere numerico, uno maiuscolo e uno speciale e non basarla su informazioni facilmente deducibili, quali il proprio nome, il nome dei famigliari, la data di nascita, il codice fiscale;
- mantenerla riservata e non divulgarla a terzi;
- non permettere ad altri utenti (es. colleghi) di operare con il proprio identificativo utente;
- non trascriverla su supporti (es. fogli, post-it) facilmente accessibili a terzi.

Supporti di memorizzazione dei dati

Nel caso in cui siano utilizzati supporti informatici quali floppy disk, cd-rom o nastri per la memorizzazione di dati sensibili e/o giudiziari, devono essere osservate le seguenti misure di sicurezza al fine di salvaguardare la riservatezza dei dati:

- i supporti informatici devono essere conservati in un luogo sicuro al fine di evitare accessi non autorizzati e trattamenti non consentiti;
- i supporti informatici se non utilizzati devono essere distrutti o resi inutilizzabili;
- i supporti informatici possono essere riutilizzati solo dopo aver provveduto a cancellare i dati e le informazioni in essi contenute; l'operazione deve essere fatta in modo che i dati precedentemente memorizzati non siano tecnicamente ed in alcun modo recuperabili. Se l'operazione non è possibile è necessario distruggere i supporti.

Protezione dei computer portatili

Un computer portatile presenta maggiori vulnerabilità rispetto ad una postazione di lavoro fissa. Premesso che quanto indicato ai paragrafi precedenti è da adottarsi anche per i computer portatili, vengono di seguito illustrate le ulteriori precauzioni che devono essere osservate nell'utilizzo di tali strumenti:

- conservare in un luogo sicuro il computer portatile a fine giornata lavorativa
- non lasciare mai incustodito il computer portatile in caso di utilizzo in ambito esterno alla ns. organizzazione;
- in caso di smarrimento e/o furto provvedere immediatamente a sporgere regolare denuncia alla competente autorità giudiziaria ed inviarne copia al nostro responsabile trattamento dati - inoltre, occorre comunicare a questi ultimi quali dati aziendali erano contenuti nel computer portatili
- rendere disponibile, qualora l'amministratore di sistema o il responsabile trattamento dati ne facciano richiesta, il computer portatile.

Attività di verifica

La nostra organizzazione per motivi tecnici e di sicurezza ed, in particolare, per prevenire o curare malfunzionamenti, può effettuare, in caso di necessità, un'analisi in tempo reale delle componenti di traffico (*file di log*) riferite alle postazioni di lavoro che accedono alla rete.

Utilizzo posta elettronica

La nostra organizzazione adotta le tecnologie dell'informazione e della comunicazione nei rapporti interni ed, in particolare, mette a disposizione del personale e di eventuali consulenti esterni indirizzi di posta elettronica individuale e/o d'ufficio.

Il servizio di posta elettronica costituisce uno strumento di lavoro e deve essere di regola utilizzato per lo svolgimento di attività strettamente connesse agli incarichi lavorativi. Nell'uso del servizio di posta elettronica, devono osservare le seguenti norme comportamentali:

- non è consentito l'utilizzo della posta elettronica della nostra organizzazione per la partecipazione a dibattiti, forum, mailing-list, ecc., attivate sia internamente che

esternamente all'organizzazione che determinano un sovraccarico della rete e creano disservizi a tutti gli utenti;

- non è consentito, per nessuna ragione, lo scambio e l'archiviazione di messaggi di posta elettronica idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale nonché lo stato di salute e la vita sessuale proprie e/o di terzi;
- è espressamente vietato l'uso di linguaggio o di immagini oscene, ingannevoli, diffamatorie, discriminatorie e/o comunque idonee;
- non è consentito spedire o rispedire posta che contenga materiale pubblicitario;
- è illecito scambiare messaggi sotto mentite spoglie, ossia impersonando un mittente diverso da quello reale;
- si raccomanda di aprire gli allegati di tipo "eseguibile" solo in caso di certezza assoluta del mittente;
- per quanto riguarda l'origine dei messaggi di posta, è opportuno considerare che è facile impersonare un mittente diverso da quello reale, soprattutto per i generatori di messaggi fraudolenti o limitare la dimensione del messaggio inviato, soprattutto nei casi in cui vi siano più destinatari. Un allegato di dimensioni eccessive potrebbe impedire l'arrivo del messaggio o richiedere un uso eccessivo delle risorse allo scopo di conseguire un più efficace impiego del servizio di posta elettronica, e nel contempo non sovraccaricare i relativi sistemi di sicurezza, si deve gestire la casella di posta elettronica, la cui i dimensione è stabilita in funzione delle necessità operative, in modo opportuno eliminando i messaggi non necessari, contenendo la dimensione degli stessi e dei relativi allegati
- mantenere riservata la password di accesso al servizio di posta elettronica, provvedendo a modificarla almeno ogni 6 mesi o ogni 3 nel caso in essa vi siano dati sensibili o giudiziali;

Disponibilità dei messaggi di posta elettronica

Il personale della nostra organizzazione, in caso di assenza programmata (ad es. per ferie o attività di lavoro fuori sede), deve adottare le misure organizzative più idonee ad assicurare la corretta gestione dei messaggi necessari al normale svolgimento dell'attività lavorativa ed alla conseguente continuità della stessa.

Nel caso, invece, di eventuale assenza improvvisa e/o prolungata (ad es. per malattia) ed il lavoratore non possa attivare la procedura sopra descritta, la nostra organizzazione si riserva la possibilità di attivare analogo accorgimento, avvertendo gli interessati.

Nel caso in cui si preveda la possibilità che, in caso di assenza improvvisa o prolungata, e per improrogabili necessità legate all'attività lavorativa, si debba conoscere il contenuto dei messaggi di posta elettronica o di altri dati aziendali che siano nella esclusiva disponibilità del dipendente, il Responsabile trattamento dati, in qualità di fiduciario, può richiedere all'amministratore di sistema che venga effettuato il reset della password dell'utente stesso. Di tale attività deve essere redatto, a cura del suddetto Responsabile, apposito verbale e deve essere informato l'utente interessato alla prima occasione utile in modo tale da metterlo in condizione di cambiare la password.

Attività di verifica della posta elettronica

L'amministratore di sistema per motivi tecnici e di sicurezza ed, in particolare, per prevenire o curare malfunzionamenti effettua una registrazione delle componenti di traffico (*file di log)* riferiti alla posta elettronica. In particolare, La nostra organizzazione effettua una temporanea registrazione delle componenti dei *file di log (*data, ora, destinatario, mittente, ecc..*)*, il cui accesso è consentito al solo personale, interno ed esterno, autorizzato alla gestione tecnica del servizio di posta elettronica.

Per quanto riguarda il contenuto dei messaggi di posta elettronica, il sistema prevede una registrazione e conservazione degli stessi garantendone la riservatezza, l'integrità e la disponibilità nel rispetto della normativa vigente.

Uso di Internet

Relativamente ai servizi internet, La nostra organizzazione ha concordato l'accesso ad internet al personale ed ai consulenti esterni. Tale accesso di regola deve avvenire per il perseguimento di finalità strettamente connesse agli incarichi lavorativi e comunque nel rispetto delle regole di seguito descritte. Nell'uso dei servizi internet devono osservare le seguenti norme comportamentali:

- presentarsi sempre con il proprio nome, mai sotto il nome altrui;
- non registrarsi a siti i cui contenuti non siano legati all'attività lavorativa;
- ricordarsi che quando si scarica del materiale da internet, spesso ne viene coinvolto il diritto di proprietà intellettuale e, pertanto, è necessario ottenere esplicita autorizzazione dall'amministratore di sistema;
- non trasferire sul proprio computer (download) file da siti sconosciuti e comunque solo per ragioni connesse all'attività lavorativa;
- non partecipare, per motivi non professionali, a forum, chat line, ecc.
- è vietato l'utilizzo di siti tipo facebook ed altri simili;
- non scaricare e non usare software gratuito o shareware prelevato da siti internet, salvo i casi in cui ciò sia necessario per lo svolgimento delle proprie mansioni;
- nel caso di esigenza a scaricare file che richiedono la tassa di registrazione, è necessario richiedere esplicita autorizzazione scritta al proprio Responsabile.

Attività di verifica uso Internet

L'amministratore di sistema per motivi tecnici e di sicurezza ed, in particolare, per prevenire o curare malfunzionamenti effettua una registrazione delle componenti (*file di log)* riferiti al traffico Internet.

In particolare, La nostra organizzazione effettua una temporanea registrazione delle richieste di navigazione ad internet senza che si possa individuare il singolo utente.

Inoltre, al fine di ridurre il rischio di usi impropri della "navigazione" in internet, ha adottato le seguenti misure:

- individuazione di categorie di siti considerati correlati o meno con la prestazione lavorativa ed eventuale blocco della possibilità di accesso agli stessi;
- configurazione di sistemi o utilizzo di filtri che prevengano, quali l'upload o l'accesso a determinati siti e/o il download di file o software aventi particolari caratteristiche (es. dimensionali o di tipologia di dato).

16 ottobre 2014
Data

Il titolare del trattamento

Data	*Nome e cognome*	*Firma di presa visione*