DISCIPLINARE INTERNO
Utilizzo e controllo degli strumenti di lavoro / servizi di posta elettronica e internet

1. PRINCIPI

1.1 Il presente documento (di seguito "*Disciplinare*") regolamenta:
- l'utilizzo degli strumenti tecnici e informatici (postazioni di lavoro fisse e mobili, apparecchi telefonici aziendali fissi e mobili, di seguito anche "*Strumenti*") che l'Istituto Primo Levi mette a disposizione e/o assegna al personale;
- l'utilizzo dei servizi di posta elettronica e di accesso a internet nell'ambito della struttura informatica dell'Istituto (di seguito anche "*Servizi*").

In questo contesto, è necessario definire le modalità di operatività e di accesso ai sistemi informativi onde assicurare, nel rispetto dei principi e delle norme vigenti in materia, la funzionalità e il corretto impiego delle varie risorse da parte degli utenti, specificando al contempo le misure adottate per garantire la disponibilità e l'integrità dei sistemi informativi stessi e dei dati ivi contenuti, nonché prevenire eventuali utilizzi impropri dei vari strumenti/servizi.

1.2 Il presente Disciplinare ottempera ai principi generali in materia di protezione dei dati personali, alla disciplina di settore che regola i rapporti di lavoro, nonché ai principi di finalità, di necessità, di correttezza, di pertinenza e non eccedenza, di cui al Codice Privacy (d.lgs. 196/2003), al Regolamento (UE) 2016/679 (GDPR) e alle Linee guida del Garante per la Protezione dei Dati Personali, di cui al Provvedimento a carattere Generale del 1 marzo 2007 (in Bollettino n. 81/marzo 2007, registro delle Deliberazioni, Delibera n. 13 del 1 marzo 2007 "Linee guida del Garante per posta elettronica e Internet").

2. CAMPO DI APPLICAZIONE

Il presente Disciplinare si applica a tutto il personale. Le disposizioni si estendono a tutti coloro che, in qualità di utenti esterni, gestiscono e utilizzano gli Strumenti/Servizi forniti dall'Istituto (di seguito "*Utilizzatori*").

3. SCOPO

Scopo del presente Disciplinare è assicurare che:

1. gli Utilizzatori degli Strumenti e dei Servizi dell'Istituto siano informati sulle modalità di operatività e di accesso, nonché sulle disposizioni vigenti in relazione alla disciplina dell'utilizzo degli Strumenti e dei Servizi stessi, anche nell'ambito dell'informativa art. 13 d.lgs. 196/03 e art. 13 e ss. GDPR;
2. gli Strumenti di lavoro e i servizi di posta elettronica e di accesso ad internet vengano utilizzati secondo quanto previsto dalla normativa di riferimento e in conformità a quanto disposto dal presente Disciplinare;

3. gli Utilizzatori degli Strumenti di lavoro e dei servizi di posta elettronica e di accesso ad internet siano informati in merito ai concetti di sicurezza e di controllo applicabili agli Strumenti e ai Servizi stessi.

4. PRESCRIZIONI INTERNE E MISURE ORGANIZZATIVE SULLA SICUREZZA DEI DATI E DEI SISTEMI; RELATIVI CONTROLLI

4.1 L'Istituto stabilisce le seguenti prescrizioni interne in materia di misure minime e idonee di sicurezza dei dati:

a) le postazioni di lavoro fisse e mobili (apparecchi telefonici fissi e cordless, pc fissi e portatili, notebook, tablet, smartphone) costituiscono strumenti di lavoro. Dette apparecchiature devono essere custodite con cura e diligenza e devono essere utilizzate esclusivamente per motivi di lavoro. Gli strumenti di lavoro assegnati a un Utilizzatore sono di pertinenza dello stesso e utilizzabili esclusivamente dall'Utilizzatore assegnatario;
b) gli strumenti di lavoro pc fissi e portatili, notebook, tablet, smartphone sono utilizzabili mediante profilo utente costituito dal binomio user-id/password, che deve essere inserito, a scelta dell'Utilizzatore, con le cautele necessarie per conservarne la segretezza e deve essere periodicamente modificato;
c) l'accesso ai sistemi informativi e ai servizi dell'Istituto (tra i quali anche i servizi internet, e di posta elettronica) avviene tramite l'informativa di credenziali identificative, che vengono fornite dall'Istituto;
d) non è consentito agli Utilizzatori di intervenire in alcun modo per modificare le caratteristiche *hardware* e *software* impostate sugli strumenti di lavoro, salvo specifica autorizzazione dell'Istituto;
e) in caso di furto o smarrimento degli strumenti di cui alla predetta lettera a), l'Utilizzatore al quale gli strumenti sono stati assegnati, oltre a denunciare l'accaduto all'Autorità di Pubblica Sicurezza, deve darne immediata notizia, con ogni mezzo, all'Istituto;
f) ogni Utilizzatore è tenuto ad assumere comportamenti volti a ridurre il rischio di accesso abusivo ai dati e di attacchi al sistema informativo. In caso di incidente informatico (vale a dire in presenza di un evento che abbia come conseguenza l'alterazione del normale funzionamento dello strumento di lavoro) oppure in presenza di *malware*, l'Utilizzatore è tenuto a scollegare l'apparato dalla rete e a darne immediata informativa al Responsabile ICT.

4.2 L'Istituto si avvale di sistemi che hanno la finalità di garantire la sicurezza nel trattamento dei dati e di tutelare la rete e i servizi da attacchi esterni, nonché per finalità di controllo e programmazione dei costi (verifica costi di connessione internet e traffico telefonico).
Gli addetti del settore ICT compiono interventi sul sistema informatico diretti a garantire la salvaguardia del sistema stesso, nonché per motivi tecnici e/o manutentivi.
Gli Utilizzatori sono codificati mediante profili di accesso alla rete di Istituto, a internet e alla casella di posta elettronica, che identificano l'utente a sistema durante l'utilizzo dei servizi e tracciato il passaggio delle attività (ad esempio *log tracer*). In particolare, possono essere tracciati dai sistemi informatici i passaggi durante l'utilizzo dei servizi di accesso a internet e alla casella di posta elettronica. Per ogni utente vengono registrati i riferimenti (indirizzi) dei siti visitati e delle pagine Web consultate. Per ogni utente vengono registrate le e-mail in uscita e in entrata

nell'ambito della propria casella di posta elettronica, senza visualizzarne il contenuto. Per ogni apparecchio telefonico vengono registrati i numeri in entrata e uscita.
Le informazioni di cui sopra possono formare oggetto di analisi da parte dell'Istituto per necessità connesse all'attività. Eventuali controlli non sono sistematici né continuativi, ma solo circostanziati e dettati da valutazioni a carattere generale, senza mai mirare a un controllo a distanza degli Utilizzatori. Controlli puntuali e nel dettaglio saranno effettuati solo in caso di perdurante anomalie del sistema informatico e/o in presenza di abusi e illeciti utilizzi, ovvero se richiesti dalle forze dell'ordine per controlli e/o in esecuzione di provvedimenti emessi da parte dell'Autorità Giudiziaria. I controlli saranno effettuati secondo il principio di gradualità.
L'Istituto, nell'esercizio della tutela dei propri beni e della propria immagine tramite i controlli di cui, sopra garantisce i diritti sanciti dallo Statuto dei Lavoratori (art. 4, come modificato dall'art. 23 del d.lgs. 151/2015, e art. 8 della L. 300 del 20/05/1970), nonché artt. 113 e 114 del Codice della Privacy).

4.3 L'Istituto potrà altresì avvalersi di un sistema di URL screening, software che consente di regolare l'utilizzo di internet. Il sistema in questione utilizza un data base che classifica i siti web e, attraverso l'applicazione di filtri, impedisce l'accesso a siti non autorizzati e inseriti in apposita lista (*black list*).
Il traffico internet potrà essere monitorato tramite un server Proxy, che registra, nel rispetto delle disposizioni di legge in materia, le attività sull'uso del servizio internet. Tali registrazioni vengono cancellate periodicamente.

5. POSTA ELETTRONICA

5.1 La casella di posta elettronica assegnata all'Utilizzatore è uno strumento di lavoro. Gli Utilizzatori delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse.
Non è consentito utilizzare la casella di posta elettronica assegnata nel dominio ***primolevi-bs.edu.it*** a fini privati o personali. L'indirizzo di posta elettronica (e-mail), ancorché riporti il nome / cognome dell'utente, è di proprietà dell'Istituto e costituisce uno strumento di lavoro; l'Istituto può quindi accedere alle comunicazioni di posta elettronica di natura professionale dei propri dipendenti e collaboratori, come qui di seguito regolato.
È fatto divieto a tutti gli Utilizzatori di fruire del servizio di posta per inviare messaggi dannosi, offensivi o sconvenienti, e comunque che siano idonei a recare un pregiudizio, anche all'immagine e al buon nome dell'Istituto.
È inoltre vietato l'uso della casella di posta per l'invio di messaggi personali o per la partecipazione a dibattiti, forum o mail-list, così come non è consentito l'utilizzo dell'indirizzo di posta per l'iscrizione a siti web di qualsiasi natura (social forum, blog ecc.), a meno di quelli necessari per il lavoro d'ufficio.
È obbligatorio controllare i file attachments di posta elettronica prima del loro utilizzo.
Si applicano all'utilizzo della posta elettronica le regole ordinarie di riservatezza e di segreto per ragioni d'ufficio; i documenti e le comunicazioni possono essere inviati/inoltrate a indirizzi di posta elettronica esterni solo per ragioni strettamente collegate ad attività lavorativa.

5.2. In caso di cessazione del rapporto, la casella di posta elettronica sarà disattivata.

6. ACCESSO E UTILIZZO DI INTERNET

Le apparecchiature assegnate al singolo Utilizzatore e abilitate alla navigazione internet costituiscono uno strumento di Istituto utilizzabile esclusivamente per lo svolgimento dell'attività lavorativa. È assolutamente proibita la navigazione in internet per motivi diversi da quelli strettamente legati all'attività lavorativa stessa. In questo senso, a titolo puramente esemplificativo, l'utente non potrà utilizzare internet per:
- accedere a siti web aventi carattere non professionale.
- accedere a servizi FTP e/o P2P vari (protocolli per il trasferimento dati) che non facciano capo a indirizzi di Istituto (ad esempio è vietato accedere a Emule e similari);
- eseguire download di file eseguibili o documenti da siti Web o Ftp non conosciuti;
- l'effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti on-line e simili, fatti salvi i casi direttamente autorizzati dall'Istituto e comunque nel rispetto delle normali procedure di acquisto connesse con l'attività di Istituto;
- ogni forma di registrazione a siti i cui contenuti non siano strettamente legati all'attività lavorativa;
- la partecipazione a Forum non professionali, l'utilizzo di chat line (esclusi gli strumenti autorizzati), di bacheche elettroniche e le registrazioni in guest books anche utilizzando pseudonimi (o nicknames) se non espressamente autorizzati.

7. UTILIZZO DEGLI APPARECCHI TELEFONICI FISSI O MOBILI, FAX E FOTOCOPIATRICI

7.1 Il telefono fisso è uno strumento di lavoro. Ne viene concesso l'uso esclusivamente per lo svolgimento dell'attività lavorativa, non essendo quindi consentite comunicazioni a carattere personale o comunque non strettamente inerenti l'attività lavorativa stessa.
7.2 È vietato l'utilizzo delle fotocopiatrici per fini personali.

L'atto autorizzativo e le istruzioni al trattamento sono presenti in area pubblica della *privacy* sul sito di Istituto.

Brescia, 13 novembre 2023