POLICY PER L'UTILIZZO
DEGLI STRUMENTI ICT
(*Information and Communication Technology*)

Indice

Introduzione

Il presente documento interno ha l'obiettivo di definire l'ambito di applicazione, le modalità e le norme sull'utilizzo della strumentazione informatica di IC Marco Polo Senago da parte degli utenti assegnatari (dipendenti, collaboratori, etc., si veda *infra*, par. 2), con le relative conseguenze in tema di responsabilità, al fine di tutelare i beni aziendali ed evitare condotte inconsapevoli e/o volutamente scorrette che potrebbero esporre IC Marco Polo Senago a problematiche di natura patrimoniale e penale oltre a rischi di sicurezza e di immagine anche per eventuali danni cagionati a terzi.

Vista la crescente diffusione delle nuove tecnologie informatiche e, in particolare, il libero accesso alla rete internet dai personal computer e, posto che l'utilizzo delle risorse informatiche e telematiche deve sempre ispirarsi al principio della diligenza e correttezza come comportamenti che normalmente si adottano nell'ambito dei rapporti di lavoro e che tutte le strumentazioni ICT (*Information and Communication Technology*) fornite da IC Marco Polo Senago agli utenti, devono essere utilizzate in modo appropriato, efficiente, rispettoso e per motivi lavorativi, la DS dell'IC Marco Polo Senago ha ritenuto opportuno stilare un insieme di norme comportamentali volte a conformare la società ai principi di diligenza, informazione e correttezza nell'ambito dei rapporti di lavoro, con l'ulteriore finalità di prevenire eventuali comportamenti illeciti dei dipendenti, pur nel rispetto dei diritti ad essi attribuiti dall'ordinamento giuridico italiano.

Considerando poi che IC Marco Polo Senago al fine di uno svolgimento più agevole delle proprie attività, mette a disposizione dei propri utenti che ne necessitano per la tipologia di funzione svolta, anche dispositivi portatili quali smartphones per il byod*, tablet o pc, sono state ivi inserite alcune clausole relative alle modalità e ai doveri cui ciascun utente deve necessariamente adeguarsi nell'utilizzo di detta strumentazione.

1. Ambito di applicazione oggettivo: definizione di strumenti ICT

Le strumentazioni ICT, messe a disposizione da IC Marco Polo Senago e oggetto di tutela da parte della presente policy, sono:

- i servizi informatici erogati;
- le postazioni di lavoro “fisse” (PC desktop e simili) e “mobili” (PC portatili, tablet e simili);
- i dispositivi cellulari (smartphones); *secondo il regolamento scolastico
- i software di comunicazione (posta elettronica e simili);
- software di lavoro;
- i server, le apparecchiature e tutto il materiale hardware in generale.

I beni, gli strumenti informatici -sia hardware che software- e le reti informatiche costituiscono patrimonio sociale e sono da considerarsi di esclusiva proprietà di IC Marco Polo Senago Il loro utilizzo, pertanto, è consentito solo per finalità di adempimento delle mansioni lavorative affidate ad ogni utente in base al rapporto in essere (ovvero per scopi professionali afferenti all’attività svolta per l’istituto), e comunque per l’esclusivo perseguimento degli obiettivi aziendali.

A tal fine si precisa sin d’ora che qualsivoglia dato e/o informazione trattato per mezzo dei beni e delle risorse informatiche è anch’esso di proprietà di IC Marco Polo Senago, è considerato di natura aziendale e non riservata.

2. Ambito di applicazione soggettivo

Il presente disciplinare interno si applica ad ogni “utente” assegnatario di beni e risorse informatiche aziendali ovvero utilizzatore di servizi e risorse informatiche di pertinenza della società.

In particolare, per "utente" si intende:

- ciascun soggetto che abbia un rapporto di lavoro subordinato con IC Marco Polo Senago, a qualsiasi titolo inserito nell'organizzazione scolastica, senza distinzione alcuna di ruolo e/o livello;
- dipendenti e collaboratori di società che hanno un contratto in essere con IC Marco Polo Senago e che possano utilizzare risorse informatiche della stessa;
- ospiti dell'azienda per eventuale utilizzo delle stesse.

3. Finalità

Il presente documento si prefigge di tutelare le risorse ICT dell' IC Marco Polo Senago e di fornire indicazioni agli utenti, come precedentemente definiti, circa il corretto ed appropriato uso delle stesse.

L'istituto, in particolare, intende perseguire i seguenti obiettivi:

- prevenire il danneggiamento, la perdita o il furto dei beni aziendali;
- ridurre i rischi relativi alle minacce di sicurezza informatica, preservando la disponibilità, integrità e confidenzialità dei dati e la continuità dei servizi erogati;
- garantire il rispetto delle normative in materia di trattamento dati, di proprietà industriale e diritto d'autore;
- prevenire la commissione dei reati c.d. presupposto, ai sensi del D. lgs. 231/2001.

4. Contesto normativo di riferimento

A tal fine, la presente policy aziendale fa riferimento al seguente complesso normativo:

- "Regolamento UE 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE" (GDPR);

- D. Lgs. 30 giugno 2003, n. 196 “Codice in materia di protezione dei dati personali” così come novellato dal D. Lgs. 10 Agosto 2018, n. 101;
- Legge 20 Maggio 1970, n. 300 (c.d. Statuto dei Lavoratori) alla luce delle ultime modifiche intervenute ad opera del D. Lgs. 14 settembre 2015, n. 151;
- Provvedimenti del Garante per la protezione dei dati personali;
- Linee Guida del WP Art. 29;
- Legge 22 Aprile 1941, n. 633 “Legge sul diritto d’autore”;
- D. Lgs. 8 Giugno 2001, n. 231.

5. Accesso a sistemi e dispositivi

L’accesso a tutti i servizi deve avvenire previa procedura di autenticazione.

Gli utenti devono essere identificati e ricevere dall’amministratore di sistema dell’IC Marco Polo Senago dal gestore del servizio le proprie credenziali individuali (nome utente e password), che devono essere mantenute riservate e custodite con cura. Ogni password deve essere associata esclusivamente ad un unico soggetto identificato. Non possono essere assegnate credenziali già utilizzate, neppure in tempi diversi, ad utenze nuove.

La password di accesso deve essere cambiata obbligatoriamente da ogni utente al primo accesso. Gli utenti devono proteggere con cura e diligenza le credenziali dei dispositivi e di tutti i sistemi informatici dell’azienda (ad es. posta elettronica, intranet, software ecc.) e, nel caso di furto o smarrimento, oltre alla segnalazione alla Dirigente Scolastica (si veda par. 8) deve provvedere nel più breve tempo possibile e senza ingiustificato ritardo al reset e alla modifica della stessa.

6. Protezione dei sistemi ICT

Per proteggere i dispositivi dalle intrusioni di virus, locker o altri sistemi infettanti sono stati installati e vengono aggiornati periodicamente antivirus e firewall adeguati alle caratteristiche delle strutture stesse.

La posta elettronica filtra anche potenziali mail di spam.

La scansione dell'antivirus va a bloccare i dati potenzialmente pericolosi presenti sulle chiavette USB e eventuali dischi esterni che vengano a contatto con un dispositivo, lo fanno in modo trasparente.

7. Criteri di utilizzo delle risorse informatiche e responsabilità

Il presente regolamento vuole rivolgersi dunque a tutte le categorie di soggetti che potenzialmente accedono ai servizi, sia ai meri utilizzatori sia a coloro che svolgono mansioni tecniche più avanzate.

Ciascun utente è personalmente responsabile dell'utilizzo dei beni e delle risorse informatiche affidatigli dall'istituto. A tal fine ogni utente, nel rispetto dei principi di diligenza sottesi al rapporto instaurato con dell'istituto è tenuto a tutelare (per quanto di propria competenza) il patrimonio aziendale da utilizzi impropri e non autorizzati, danni o abusi anche derivanti da negligenza, imprudenza o imperizia.

L'obiettivo è quello di preservare l'integrità e la riservatezza dei beni, delle informazioni e delle risorse dell'istituto.

Al di là delle modalità di trattamento, sulle quali si approfondisce nei paragrafi successivi, è espressamente vietato pertanto, attraverso qualsiasi forma, comunicare a terzi non inerenti all'IC Marco Polo Senago informazioni, con o senza scopo di lucro, che riguardino il *know-how*della scuola.

7.1 Risorse hardware e software

In generale, su tutte le risorse hardware e software è fatto assoluto divieto di:

- apportare modifiche degli strumenti, togliendo, sostituendo o inserendo componenti *ex novo*, senza previa richiesta e autorizzazione del Referente dei sistemi informatici;
- apportare modifiche ai parametri di configurazione originaria dei dispositivi, installare, disinstallare, scaricare nuovi software; sono fatte salve tutte quelle modifiche di pura personalizzazione a livello di utenza che non abbiano conseguenze negative sulle funzionalità dei dispositivi stessi;
- creare copie (anche parziali) di software protetti dal diritto d'autore.

Nell'utilizzo dei già menzionati strumenti, gli utenti sono tenuti a:

- sottoporre a scansione preventiva gli eventuali supporti mobili da inserire del dispositivo, quali, ad esempio, pendrive USB, CD-ROM, DVD, hard-disk esterni, e altri);
- bloccare i dispositivi nel caso in cui non possano essere presidiati (durante le pause in generale e ogniqualvolta ci si dovesse allontanare dalla postazione di lavoro);
- non trasportare al di fuori della sede dell'IC Marco Polo Senago postazioni di lavoro fisse, salvo specifica autorizzazione;
- non mantenere abilitati protocolli insicuri di trasmissione dati, come il Bluetooth, oltre il tempo strettamente necessario;
- procedere allo spegnimento delle postazioni al termine dell'orario di lavoro, fatto salvo particolari richieste per esigenze autorizzate dal Referente di riferimento che avrà, a sua volta, chiesto al Referente dei servizi informatici.

7.2 Dispositivi portatili e smartphones (si veda il regolamento di istituto che norma il Bring your own device)

Fatte salve le regole generali indicate al punto precedente, l'utilizzo di dispositivi portatili e degli smartphones, all'esterno dei locali dell'azienda, deve essere oggetto di particolare cura ed attenzione da parte degli utenti perché tale utilizzo rappresenta una fonte di rischi particolarmente rilevante in termini di sicurezza, sia delle risorse in sé sia dei dati nelle stesse contenuti.

Tali dispositivi, infatti, possono essere maggiormente soggetti a smarrimento, furti, distruzione o compromissione dei dati, tentativi di frode e/o accesso non autorizzato ovvero essere "infettati" da virus o codice malevole.

Peraltro, un'eventuale contaminazione da virus informatici potrebbe diffondersi e ripercuotersi all'intera rete informatica della società, una volta che tali dispositivi siano collegati direttamente alla rete interna. A tal fine, particolare attenzione deve inoltre essere posta nell'utilizzo di reti Wi-Fi esterne.

È tuttavia concesso un utilizzo personale dei dispositivi purché sporadico e moderato, con la c.d. "diligenza del buon padre di famiglia" e comunque tale da non ledere il rapporto fiduciario

instaurato con il proprio datore di lavoro.

A tal proposito, IC Marco Polo Senago informa i propri utenti che, nel caso di poca diligenza nella custodia e di danneggiamento arrecato allo strumento, provocato dall'assegnatario, l'istituto potrà richiedere il risarcimento del danno.

7.3 Posta elettronica

La posta elettronica è un mezzo di comunicazione messo a disposizione del dipendente unicamente per consentirgli lo svolgimento della propria attività lavorativa.

Si raccomanda pertanto di evitare di utilizzare tale strumento per motivi non attinenti allo svolgimento delle mansioni assegnate, salvo casi eccezionali o di comprovata urgenza e necessità.

È fatto divieto, in ogni caso, di trasmettere a chiunque tramite tale mezzo di comunicazione materiale pedo-pornografico, materiale fraudolento o illegale, gioco d'azzardo, materiale blasfemo, molesto e/o osceno.

Tale regola riguarda sia il contenuto del messaggio che eventuali suoi allegati.

A tal proposito si specifica che non è nemmeno consentito:

- utilizzare tecniche di "mail spamming", ovvero l'invio massiccio e incontrollato di comunicazioni che non siano istituzionali;
- inoltrare catene di S. Antonio, giochi, scherzi, barzellette e simili.

Il fine che IC Marco Polo Senago vuole perseguire con l'imposizione di tali regole comportamentali è preservare la struttura informatica dell'istituto e i dati in essa contenuti, nel rispetto della normativa dei diritti dei lavoratori.

Nel dettaglio, tali regole vogliono prevenire fenomeni assai frequenti di insinuazione di malware e furto dati, quali *phishing* o *whaling*.

7.4 Rete aziendale

Premesso che l'abilitazione alla navigazione è funzionale allo svolgimento dell'attività lavorativa, l'IC Marco Polo Senago, ad oggi, ha scelto di non oscurare alcun tipo di sito internet: non esistono dunque blocchi massivi di indirizzi inseriti in una black-list.

Ciò non esime l'utente dal divieto di fare un utilizzo improprio di tale risorsa, in particolare non è assolutamente consentito:

- navigare su siti proponenti pedopornografia, materiale fraudolento o illegale, gioco d'azzardo, materiale blasfemo, discriminatorio, molesto e/o osceno e, in ogni caso, contrario all'ordine pubblico;
- l'effettuazione di ogni genere di transazione finanziaria privata, ivi comprese le operazioni di remote banking, acquisti on-line e simili, salvo casi espressamente autorizzati dalla società;
- registrarsi a siti i cui contenuti non siano legati all'attività lavorativa;
- partecipare a forum, chat-line o di bacheche elettroniche, guest-book, anche utilizzando pseudonimi (o nicknames);
- lo scambio e/o la condivisione a qualsiasi titolo, anche se non a scopo di lucro, di materiale audiovisivo, cinematografico, fotografico, informatico, etc., protetto da copyright.
  Le norme contenute in questo paragrafo vogliono scongiurare il pregiudizio dell'immagine e della struttura informatica dell' IC Marco Polo Senago da tecniche di *watering hole*.

7.5 Telefoni, scanner, stampanti e fotocopiatrici

Per quanto riguarda l'utilizzo del telefono fisso, si raccomanda di limitarne l'uso alle comunicazioni lavorative, salvo casi eccezionali e avendo cura di contenere l'eventuale durata della telefonata al minimo indispensabile.

È richiesta, inoltre, una particolare attenzione quando si invia su una stampante condivisa documenti aventi ad oggetto dati personali o informazioni riservate; ciò al fine di evitare che persone non autorizzate possano venirne a conoscenza. Si richiede quindi di evitare di lasciare le stampe incustodite e ritirarne immediatamente le copie non appena uscite dalla stampa.

8. Controlli

Si vuole innanzitutto premettere che qualsiasi controllo attuato da l'IC Marco Polo Senago per i fini di cui al presente documento è svolto sull'uso degli strumenti ICT secondo le prescrizioni

dell'art. 4 della L. 20 Maggio 1970, n. 300 (c.d. Statuto dei Lavoratori) e del nuovo Regolamento UE 2016/679 sulla protezione dei dati personali delle persone fisiche: è quindi nel pieno rispetto dei principi di pertinenza e di non eccedenza ed evitando ogni interferenza ingiustificata sui diritti e sulle libertà fondamentali dei lavoratori.

La prima fase di controllo sull'utilizzo delle strutture ICT e dei dati con esse trattati spetta ai Referenti di concerto con il Referente informatico e la Dirigente Scolastica, i quali sono tutti tenuti a garantire l'adozione delle prassi ivi descritte.

Vi è poi una seconda fase di controllo che riguarda la possibilità di accesso da parte dell'amministratore di sistema alle informazioni relative a dati, sistemi, azioni, reti ed applicazioni utilizzati, raccolte dai log di sistema.

Si rende noto in primo luogo che detti controlli sono sporadici, indiretti e di tipo aggregato, finalizzati a verificare la funzionalità e la sicurezza dei sistemi. Per quanto possibile deve essere preferito un controllo preliminare su dati aggregati, riferiti all'intera struttura lavorativa o a sue aree. Il controllo anonimo può concludersi con un avviso generalizzato relativo ad un rilevato utilizzo anomalo degli strumenti aziendali e con l'invito ad attenersi scrupolosamente a compiti assegnati e istruzioni impartite.

Controlli indiretti di tipo aggregato, ma più specifici, vengono altresì attivati in caso di rilevamento di anomalie o di danni nell'utilizzo delle apparecchiature ICT. Qualora, poi, l'anomalia dovesse ripetersi e riguardare lo stesso ambito lavorativo si procederà con l'effettuazione di controlli più puntuali e su base individuale.

In assenza di successive anomalie non è di regola giustificato effettuare controlli su base individuale.

9. Gestione degli incidenti e *Data Breach*

Ogni incidente (ad es. malfunzionamento PC, indisponibilità dei servizi applicativi e di rete, perdita o furto di un *device*) deve essere segnalato dall'utente in modo tempestivo al proprio Referente e al Referente delle infrastrutture informatiche, i quali, di concerto con le altre figure apicali aziendali, nel più breve tempo possibile e per le rispettive competenze, raccoglieranno le segnalazioni e avvieranno il relativo processo di classificazione e risoluzione dell'incidente medesimo al fine di minimizzare gli eventuali impatti negativi sui dati oggetto dell'incidente e sul normale svolgimento delle attività lavorative.

In particolare, l'utente, nei casi di smarrimento, furto accertato o grave manomissione dei dispositivi assegnati o del loro contenuto deve segnalare tempestivamente l'accaduto ai soggetti di

seguito indicati:

- Autorità Giudiziaria (sporgendo denuncia);

- Referente informatico aziendale e Referente ufficio acquisti, per l'eventuale blocco dell'uso delle risorse ICT.

Per gli incidenti che possono determinare anche una violazione dei dati personali, cioè la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati (cd. "*Data Breach*"), l'art. 33 del GDPR prevede che:

"In caso di violazione dei dati personali, il Titolare del trattamento notifica la violazione all'Autorità di controllo competente a norma dell'articolo 55 senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche.

Qualora la notifica all'Autorità di controllo non sia effettuata entro 72 ore, è corredata dei motivi del ritardo. [*omissis*]

La notifica di cui al paragrafo 1 deve almeno:

a) descrivere la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;

b) comunicare il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;

c) descrivere le probabili conseguenze della violazione dei dati personali;

d) descrivere le misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

Qualora e nella misura in cui non sia possibile fornire le informazioni contestualmente, le informazioni possono essere fornite in fasi successive senza ulteriore ingiustificato ritardo.

Il Titolare del trattamento documenta qualsiasi violazione dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio. Tale documentazione consente all'Autorità di controllo di verificare il rispetto del presente articolo".

Il successivo art. 34 disciplina, poi, il caso in cui la violazione dei dati personali sia suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche: in tal caso è necessario comunicare l'avvenuta violazione all'interessato senza ingiustificato ritardo, a meno che non si verifichino le circostanze indicate nel paragrafo 3 dell'articolo, ovvero:

"a) il Titolare del trattamento ha messo in atto le misure tecniche e organizzative adeguate di

protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura;

b) il Titolare del trattamento ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati;

c) detta comunicazione richiederebbe sforzi sproporzionati. In tal caso, si procede invece a una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia".

10. Sanzioni

L'eventuale violazione di quanto previsto dal presente disciplinare interno – rilevante anche ai sensi degli art. 2104[1] e 2105[2] c.c. - potrà comportare l'applicazione agli utenti di sanzioni disciplinari in base a quanto previsto dall'art. 7 dello Statuto dei Lavoratori, oltre all'applicazione in capo ai contravventori di sanzioni di tipo civile e/o penale, a cui, per quanto qui non espressamente previsto o richiamato, si fa esplicito rimando.

L'istituto avrà cura di informare senza ritardo (e senza necessità di preventive contestazioni e/o addebiti formali) le Autorità competenti, nel caso venga commesso un reato, o la cui commissione sia ritenuta probabile o solo sospettata, tramite l'utilizzo illecito o non conforme dei beni e degli strumenti informatici aziendali.

Si precisa, infine, che in caso di violazione accertata da parte degli utenti delle regole e degli

---

[1] *Diligenza del prestatore di lavoro* – "Il prestatore di lavoro deve usare la diligenza richiesta dalla natura della prestazione dovuta, dall'interesse dell'impresa e da quello superiore della produzione nazionale.

Deve inoltre osservare le disposizioni per l'esecuzione e per la disciplina del lavoro impartite dall'imprenditore e dai collaboratori di questo dai quali gerarchicamente dipende."

[2] *Obbligo di fedeltà* - Il prestatore di lavoro non deve trattare affari, per conto proprio o di terzi, in concorrenza con l'imprenditore, né divulgare notizie attinenti all'organizzazione e ai metodi di produzione dell'impresa, o farne uso in modo da poter recare ad essa pregiudizio."

obblighi esposti in questo disciplinare, l'IC Marco Polo Senago si riserva la facoltà di sospendere, bloccare o limitare gli accessi di un account, quando appare ragionevolmente necessario per proteggere l'integrità, la sicurezza e/o la funzionalità dei propri beni e strumenti informatici, oltre a richiedere il risarcimento dell'eventuale danno ingiustamente subito.

Del presente atto sarà fornita massima pubblicità e diffusione, anche a seguito di ogni aggiunta e modifica, tramite i diversi canali di informazione aziendale.

Documento deliberato in Consiglio di Istituto il giorno 18/01/2023