REGOLAMENTO PER L'USO DI TABLET E SMARTPHONE

Premesso che l'utilizzo delle risorse informatiche e telematiche istituzionali deve sempre ispirarsi ai principi di diligenza e correttezza, atteggiamenti questi destinati a sorreggere ogni atto o comportamento posto in essere nell'ambito del rapporto di lavoro, si ritiene utile adottare ulteriori regole interne dirette ad evitare comportamenti inconsapevoli e/o scorretti. Inoltre, questo regolamento è obbligatorio a partire dal Provvedimento dell'Autorità Garante per la Privacy del 1° marzo 2007 (Gazzetta Ufficiale n. 58 del 10 marzo 2007) e risponde anche all'esigenza di dare una corretta informativa sull'uso dei dati automaticamente ed implicitamente "trattati" a causa dell'uso di un apparato mobile (Tablet, Smartphone o Telefono cellulare).

Ai sensi del GDPR 2016/679 e della normativa nazionale vigente in materia di trattamento e protezione dei dati, ogni incaricato del trattamento, cui sia stato dato accesso al sistema informativo istituzionale mediante credenziali di autenticazione, è autorizzato all'utilizzo della strumentazione elettronica in dotazione all'Istituto (computer, stampanti, fax, scanner, fotocopiatori, dispositivi di rete, etc.) e all'utilizzo della strumentazione telefonica e di comunicazione mobile (telefoni cellulari, smartphone e tablet) per lo svolgimento dei compiti assegnati e in particolare per il trattamento dei dati personali entro il proprio ambito e secondo le istruzioni ricevute.

Il presente Regolamento integra il vigente Disciplinare interno e policy istituzionale sul trattamento dei dati.

1. Utilizzo del dispositivo mobile

1.1 Disposizioni generali

- Per "Dispositivo mobile" è da intendersi il telefono cellulare, il tablet, lo smartphone e ogni altro dispositivo che consenta la gestione di audio, video e di applicativi software "in mobilità".
- I dispositivi mobile sono in dotazione per l'uso lavorativo.
- In generale, i dispositivi mobile non possono essere ceduti né fatti utilizzare a terzi, eccetto colleghi, collaboratori, consulenti o soggetti autorizzati. In particolare, alcuni telefoni sono di uso individuale e non possono essere ceduti né fatti utilizzare neppure ai colleghi.
- Il Responsabile IT può disporre dei dispositivi mobile secondo necessità, sostituendo, aggiornando, rimuovendo o adeguando in tutto o in parte le componenti hardware e/o software di cui essi si compongono, senza necessità di preavviso e di richiesta di consenso da parte dell'utilizzatore.

- Il Responsabile IT è l'unico che può provvedere o autorizzare l'installazione, l'aggiornamento e la configurazione di dispositivi hardware e/o software sui programmi in uso, sui dispositivi mobile e più in generale sull'intero sistema telefonico e di comunicazione telematica.
- Non è consentito modificare le caratteristiche hardware e software impostate sui dispositivi mobile.
- Non è consentita l'installazione di programmi diversi da quelli autorizzati.
- Non è consentita la riproduzione, la duplicazione, il salvataggio o lo scarico (download o file sharing) di programmi o file di ogni tipo (testo, immagini, video, audio, eseguibili) in violazione delle norme sul diritto d'autore, ai sensi delle Legge n. 128 del 21 maggio 2004.
- Non è consentita l'installazione di ulteriori dispositivi rispetto a quelli in dotazione.
- Non è consentito l'uso di qualsiasi dispositivo esterno da collegare al dispositivo mobile, se non quelli istituzionali o quelli autorizzati.
- L'utilizzatore che abbia necessità di apportare modifiche software o hardware al dispositivo mobile in dotazione, installando nuovi programmi o dispositivi, deve farne preventiva richiesta al Responsabile IT.
- Quanto memorizzato sui supporti interni al dispositivo mobile potrebbe essere oggetto di analisi, controllo e duplicazione da parte del Responsabile IT o da personale tecnico autorizzato, per migliorare l'affidabilità, la disponibilità e l'efficienza del dispositivo.
- Qualora fossero individuate componenti hardware e/o software (programmi, documenti, dispositivi esterni, etc.) non corrispondenti ai criteri di sicurezza e di operatività individuati dal Responsabile IT o non esplicitamente autorizzati, tali componenti potrebbero essere rimossi e l'utilizzatore potrebbe essere coinvolto negli accertamenti e nelle verifiche del caso.

1.2 Disposizioni operative

- I dispositivi mobili devono avere abilitato il codice di blocco e/o il PIN d'accesso e/o la Password personalizzata. Tale codice d'accesso dev'essere impostato al massimo del numero di caratteri consentito dal sistema operativo dello strumento e l'eventuale password utilizzata non deve facilmente richiamare né date di nascita né altri riferimenti anagrafici. Si consiglia l'uso di password alfanumeriche composte anche di lettere maiuscole e simboli, sempre se ammessi dal sistema operativo del mobile in dotazione. La password prescelta dovrà essere comunicata al Responsabile IT istituzionale, sia al primo uso che ogni volta che si deciderà di mutarla.
- I dispositivi mobile devono essere dotati di software di *remote wiping* per cancellare i dati una volta che il dispositivo dovesse cadere in mani sbagliate. Se l'installazione di detto software non è stata fatta dall'Area IT istituzionale, dovranno essere comunicate le modalità di cancellazione remota al Responsabile IT istituzionale.
- E' fatto espresso uso di un qualsiasi software e/o tecnica di jailbreack (Apple) o root (Android), cioè di quei sistemi che consentono di modificare funzionalità del sistema

operativo di un dispositivo mobile a basso livello ed a livello di "massimo amministratore".

- Se il dispositivo mobile consente l'attivazione dei servizi di tethering ovvero consentire la configurazione dell'apparato come gateway per offrire accesso alla Rete ad altri dispositivi che ne sono sprovvisti, questo tipo di possibilità va usata solo per periodi limitati ed in assenza di ogni altra soluzione di connettività (UMTS, WiFi, Rete Ethernet, etc.). Il servizio va immediatamente disattivato al termine dell'utilizzo e va protetto da password almeno alfanumeriche.
- Il Bluetooth ed ogni altro protocollo che consenta l'associazione di dispositivi diversi dallo strumento mobile, dev'essere abilitato per l'accoppiamento ai soli strumenti istituzionali in dotazione. Inoltre può essere usato, in particolare, per l'attivazione dell'auricolare personale e/o del kit viva-voce dell'auto. Il Bluetooth non va mai lasciato inutilmente attivo e le password d'associazione non devono mai essere quelle di default previste per il dispositivo.
- E' fatto espresso divieto d'utilizzare un qualsiasi dispositivo mobile istituzionale durante la guida. L'uso in auto è consentito solo mediante kit "viva voce" e/o con auricolare.
- L'eventuale periferica WiFi va abilitata sul dispositivo mobile solo ed esclusivamente ai fini d'accesso alla rete istituzionale e/o di altre reti protette. Non va mai lasciato inutilmente attivo.
- Del dispositivo mobile deve essere fatto regolarmente un backup o attraverso specifiche istruzioni da parte dell'Area IT oppure direttamente dal Responsabile IT istituzionale o da proprio incaricato.

2. Guasto o furto

In caso di guasti o malfunzionamenti, l'utilizzatore dovrà rivolgersi al Responsabile IT a cui è demandata la relativa gestione in queste circostanze.
In caso di furto o smarrimento o danneggiamento dei dispositivi mobili, l'utilizzatore deve dare tempestiva comunicazione al Responsabile IT, rimanendo a disposizione nel caso sia necessario denunciare l'accaduto all'Autorità preposta.
Non è esclusa a priori la responsabilità dell'utilizzatore nel sostenere, anche solo in parte, i costi per la riparazione o sostituzione del dispositivo mobile.

3. Dati di traffico, GPS e tabulati telefonici

Utilizzando sistemi telefonici per esigenze produttive ed organizzative, è indispensabile l'uso di sistemi evoluti che consentono indirettamente un controllo a distanza (c.d. controllo preterintenzionale) e determinano un trattamento di dati personali riferiti o riferibili ai lavoratori, nel rispetto dello Statuto dei lavoratori (art. 4, comma 2 L. 300/1970). Tali sistemi registrano le connessioni, ovvero tengono traccia dell'ora, del dispositivo mobile (e dell'eventuale affidatario) richiedente e della risorsa richiesta e potrebbero eventualmente memorizzare il contenuto della comunicazione. Inoltre possono tener traccia, anche in

tempo reale, dell'esatta posizione e/o dei percorsi compiuti dall'utilizzatore (mediante GPS e/o software di recupero del dispositivo in caso di furto/smarrimento). A meno di particolari esigenze tecniche o di sicurezza, circoscritte comunque a periodi di tempo limitati, tali sistemi sono programmati e configurati in modo da cancellare periodicamente ed automaticamente (attraverso procedure di sovra-registrazione come, ad esempio, la cd. rotazione dei log file) i dati personali relativi agli accessi al traffico generato.
I dati di traffico acquisiti dal sistema di telefonia sono utili per la validazione dei prospetti di consumo che le compagnie telefoniche addebitano, sulla base dei tabulati telefonici da esse riscontrati; pertanto l'operazione di trattamento dei dati di traffico mira principalmente a verificare la sussistenza e la veridicità dei conti telefonici. Potrebbe emergere dall'analisi primaria un interesse ad approfondire la genesi dei costi ed eventualmente a verificare il corretto utilizzo dei telefoni istituzionali.
Pertanto, è facoltà dell'Istituto effettuare controlli mirati all'individuazione di condotte illecite o vietate, ricorrendo sia ai tabulati telefonici, sia ai dati di traffico registrati dal sistema di telefonia interno, mediante operazioni di analisi, selezione e raffronto.

4. Utilizzo della rete Internet e dei relativi servizi

4.1 Navigazione in Internet

- L'Istituto declina ogni responsabilità per l'effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, pagamenti con carte di credito e simili;
- Non è consentito lo scarico e l'installazione di software gratuiti o in versione di prova (freeware e shareware) prelevati da siti Internet, se non espressamente autorizzati dall'Area IT;
- Non è consentito lo scarico di immagini, filmati e files musicali non attinenti all'attività lavorativa ed in violazione delle leggi sul diritto d'autore.

4.2 Posta elettronica istituzionale

Nel precisare che anche la posta elettronica è uno strumento di lavoro, si ritiene utile segnalare che:

- le caselle di posta elettronica istituzionale assegnate ai dipendenti ed ai collaboratori (caselle, ad esempio, del tipo nome.cognome@dominioistituzionale.xy) possono essere utilizzate, limitatamente, anche per inviare e ricevere messaggi personali;
- la natura della corrispondenza effettuata con le caselle di posta elettronica istituzionali (caselle, ad esempio, del tipo ufficio@dominioistituzionale.xy) non è privata e non è consentito utilizzare tali caselle per motivi non attinenti allo svolgimento delle mansioni assegnate; i responsabili sono tenuti a controllare la posta in arrivo almeno una volta al giorno e devono delegare una persona di fiducia che possa farlo in caso di propria assenza;
- non è consentito inviare o memorizzare messaggi di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica;

- tutte le caselle di posta elettronica sono oggetto di salvataggio automatico sia per le comunicazioni in ingresso che in uscita.

5. Cessazione o sospensione del rapporto di lavoro

Nel caso in cui cessi il rapporto di lavoro o di collaborazione, l'utente incaricato del trattamento deve:

- consegnare i dispositivi mobile istituzionali in dotazione;
- copiare i files e i documenti elettronici di rilevanza istituzionale sul server;
- è compito dell'Area IT, in seguito alla cessazione di un rapporto di lavoro:
  - effettuare il ripristino alla configurazione iniziale (reset) dei dispositivi mobile istituzionali dotati di sistema operativo;
  - attivare un risponditore automatico sulla casella di posta elettronica precedentemente concessa in uso all'incaricato: tale sistema entrerà in funzione per la durata di 1 mese, salvo accordi diversi, e comunicherà eventuali riferimenti alternativi; al termine del periodo previsto, la casella sarà disattivata;
  - disattivare le credenziali di autenticazione sui server.

6. Controlli e tutela della privacy

Poiché in caso di violazioni contrattuali e giuridiche, sia l'Istituto, sia il singolo lavoratore sono potenzialmente perseguibili con sanzioni, anche di natura penale, l'Istituto verificherà, nei limiti consentiti dalle norme legali e contrattuali, il rispetto delle regole e l'integrità del proprio sistema informatico.

Ai sensi dell'art. 13 e 14 del GDPR 2016/679 e della normativa nazionale vigente, in conformità a quanto disposto dalla Provvedimento n. 13 del 1° marzo 2007 dell'Autorità Garante per la privacy, si ritiene necessario informare che:

- la Direzione, attraverso l'Area IT istituzionale, effettua un monitoraggio periodico dell'hardware e del software installato nei dispositivi mobile istituzionali. Tale operazione viene effettuata, in modo completamente automatico per i dispositivi ed i sistemi operativi che lo consentono ed in modo manuale per tutti gli altri. Il monitoraggio, necessario per finalità organizzative (inventario del parco macchine e contabilità delle licenze d'uso del software), non coinvolge in alcun modo i dati personali ed i documenti presenti sui dispositivi, ma permette la rilevazione di software installato in violazione di questo regolamento;
- al fine di prevenire, per quanto e ove possibile, comportamenti scorretti durante la navigazione in Internet, l'Istituto si avvale di appositi filtri che impediscono l'accesso a siti non ritenuti idonei ed il download di files multimediali non attinenti all'attività lavorativa;
- i files contenenti le registrazioni della navigazione sul web sono conservati per 6 mesi come previsto dalle norme in vigore e da esigenze di sicurezza;

- eventuali comportamenti anomali saranno segnalati genericamente alle aree interessate (uffici, servizi) e, solo qualora tali comportamenti dovessero continuare, la Direzione potrà procedere, nel rispetto delle norme legali e contrattuali, a controlli individuali;
- nessun controllo viene effettuato sui messaggi di posta elettronica il cui contenuto riguarda forme di corrispondenza assistite da garanzie di segretezza, tutelate anche dalla Costituzione e da norme penali.

Il trattamento dei dati, così come descritto, è obbligatorio, pena l'impossibilità di utilizzare qualunque dispositivo mobile.

I dati personali saranno trattati nel rispetto delle modalità indicate nel GDPR 2016/679, il quale prevede, tra l'altro, che i dati stessi siano trattati in modo lecito e secondo correttezza, raccolti e registrati per scopi determinati, espliciti e legittimi, esatti, e se necessario aggiornati, pertinenti, completi e non eccedenti rispetto alle finalità del trattamento, nel rispetto delle misure di sicurezza previste dall'art. 32 GDPR 2016/679.

I dati potranno essere comunicati in Italia e all'Estero all'interno del Gruppo Comprensivo di San Zenone degli Ezzelini e a soggetti terzi per incarichi specifici e rispondenti alle finalità del trattamento e nei casi previsti dalla legge.

Gli utenti possono esercitare i diritti di cui agli artt. dal 15 al 22 del GDPR 2016/679, tra cui conferma dell'esistenza, rettifica, integrazione e cancellazione dei dati.

Titolare del trattamento è Comprensivo di San Zenone degli Ezzelini.

La non osservanza del presente regolamento può comportare sanzioni disciplinari, civili e penali.

San Zenone degli Ezzelini, 15/07/2021

Per presa visione