COMUNE DI CALENDASCO

POLICY PER L'UTILIZZO CONSAPEVOLE DEGLI STRUMENTI INFORMATICI, DELLA POSTA ELETTRONICA E DELLA RETE INTERNET

Sommario

1. Premessa

1.1 La presente policy è adottata da:

CALENDASCO, con sede in 29010 Calendasco (PC), via G. Mazzini n. 4, codice fiscale 00216710335, in persona del legale rappresentante pro tempore, nella qualità di Titolare del trattamento (di seguito "**Titolare**" o "**Ente**").

1.2 La policy è volta a promuovere un utilizzo consapevole e responsabile degli strumenti informatici, della posta elettronica e dell'accesso a Internet messi a disposizione dall'Ente per lo svolgimento delle attività istituzionali, al fine di ridurre i rischi per la sicurezza delle informazioni e per la protezione dei dati personali trattati.

1.3 L'adozione della presente policy costituisce una misura organizzativa ai sensi dell'art. 32 del Regolamento (UE) 2016/679 (GDPR), finalizzata alla prevenzione di incidenti di sicurezza e di violazioni di dati personali connessi all'utilizzo degli strumenti informatici.

1.4 La presente policy si applica a tutto il personale che, a qualunque titolo, utilizza strumenti informatici e servizi digitali nell'ambito delle attività istituzionali dell'Ente.

2. Contesto normativo e regolamentare

2.1 La presente policy è adottata nel rispetto del quadro normativo vigente in materia di protezione dei dati personali e di sicurezza delle informazioni rilevanti ai fini del trattamento dei dati personali e, in particolare, tenendo conto:

- del Regolamento (UE) 2016/679 (GDPR);
- del D. Lgs. 30 giugno 2003, n. 196, come modificato dal D. Lgs. 10 agosto 2018, n. 101;
- delle Linee guida e degli orientamenti adottati dal Comitato europeo per la protezione dei dati (EDPB) e dall'Autorità Garante per la protezione dei dati personali;
- delle indicazioni operative elaborate da autorità nazionali competenti in materia di sicurezza informatica per le pubbliche amministrazioni.

3. Ambito di applicazione

3.1 La presente policy si applica all'utilizzo degli strumenti informatici messi a disposizione dall'Ente, quali, a titolo esemplificativo:

- postazioni di lavoro (PC fissi o portatili);
- dispositivi mobili assegnati (es. smartphone, tablet);
- sistemi di posta elettronica istituzionale;
- applicativi e piattaforme informatiche;
- accessi a reti informatiche e servizi Internet.

3.2 L'utilizzo di tali strumenti avviene nell'ambito delle attività istituzionali e comporta il trattamento di dati personali, anche appartenenti a categorie particolari.

4. Utilizzo degli strumenti informatici e dei servizi digitali

4.1 Il personale utilizza gli strumenti informatici e i servizi digitali messi a disposizione dall'Ente esclusivamente per finalità connesse allo svolgimento delle attività istituzionali, nel rispetto dei principi di sicurezza delle informazioni e di protezione dei dati personali.

4.2 L'utilizzo improprio o non consapevole degli strumenti informatici può determinare rischi per la riservatezza, l'integrità e la disponibilità delle informazioni trattate, nonché favorire il verificarsi di incidenti di sicurezza o violazioni di dati personali.

5. Utilizzo della posta elettronica istituzionale

5.1 Il sistema di posta elettronica istituzionale rappresenta uno strumento di lavoro essenziale per lo svolgimento delle attività amministrative e può comportare il trattamento di dati personali.

5.2 Il personale presta particolare attenzione:

- alla verifica dei destinatari dei messaggi prima dell'invio, soprattutto in presenza di dati personali;
- al contenuto degli allegati trasmessi;
- all'utilizzo delle funzioni di inoltro automatico;
- alla gestione dei messaggi contenenti informazioni riservate.

6. Buone pratiche per un utilizzo consapevole

6.1 Al fine di ridurre i rischi per la sicurezza delle informazioni e per la protezione dei dati personali trattati nello svolgimento delle attività istituzionali, il personale è tenuto ad adottare comportamenti improntati alla diligenza e alla prudenza nell'utilizzo degli strumenti informatici.

6.2 In particolare, si raccomanda di:

- utilizzare password robuste e non facilmente riconducibili alla propria persona, evitando di condividerle con terzi;
- bloccare la postazione di lavoro in caso di allontanamento, anche temporaneo;
- prestare attenzione a messaggi di posta elettronica sospetti o provenienti da mittenti sconosciuti, evitando di aprire allegati o collegamenti ipertestuali non verificati;

- verificare con attenzione i destinatari dei messaggi di posta elettronica prima dell'invio;
- non utilizzare dispositivi di memorizzazione esterni di provenienza incerta;
- evitare l'utilizzo di reti Wi-Fi pubbliche o non protette per l'accesso a sistemi o applicativi dell'Ente;
- non installare autonomamente software o applicazioni sui dispositivi assegnati;
- effettuare con regolarità il salvataggio dei documenti di lavoro nei sistemi messi a disposizione dall'Ente;
- segnalare tempestivamente eventuali anomalie, malfunzionamenti o sospetti incidenti di sicurezza secondo quanto previsto dalla procedura di gestione degli incidenti di sicurezza e delle violazioni di dati personali adottata dall'Ente.

7. Gestione delle stampe e delle stampe

7.1 La stampa di documenti contenenti dati personali deve essere limitata ai soli casi strettamente necessari allo svolgimento delle attività istituzionali.

7.2 Il personale è tenuto a:

- verificare la correttezza del contenuto del documento prima della stampa, in particolare in presenza di dati personali;
- ritirare tempestivamente i documenti stampati presso dispositivi condivisi;
- evitare di lasciare incustoditi documenti contenenti dati personali in prossimità delle stampanti di rete.

7.3 I documenti cartacei contenenti dati personali non più necessari devono essere eliminati mediante modalità idonee a impedirne la leggibilità o la ricostruzione, nel rispetto delle procedure interne di gestione documentale adottate dall'Ente.

8. Utilizzo di social media e strumenti di comunicazione online

8.1 L'utilizzo di piattaforme di comunicazione online (quali, a titolo esemplificativo, social network, servizi di messaggistica istantanea, forum o applicativi di condivisione di contenuti) può comportare rischi per la sicurezza delle informazioni e per la protezione dei dati personali trattati nell'ambito delle attività istituzionali.

8.2 Il personale è pertanto invitato a prestare particolare attenzione a:

- non divulgare, anche involontariamente, informazioni riservate o dati personali appresi nello svolgimento delle proprie mansioni;

- non condividere documenti, immagini, schermate o altri contenuti relativi ad attività lavorative che possano contenere dati personali o informazioni non destinate alla diffusione;
- evitare riferimenti a procedimenti amministrativi, attività interne o servizi non ancora resi pubblici;
- verificare che eventuali contenuti pubblicati non consentano l'identificazione diretta o indiretta di interessati.

8.3 Eventuali contenuti relativi ad attività dell'Ente possono essere condivisi esclusivamente se già oggetto di diffusione istituzionale o comunque autorizzati secondo le procedure interne.

9. Continuità operativa e disponibilità delle informazioni

9.1 Gli strumenti informatici e le caselle di posta elettronica istituzionali sono assegnati per finalità connesse allo svolgimento delle attività lavorative e possono contenere informazioni necessarie alla continuità operativa dell'Ente.

9.2 Il personale è tenuto ad organizzare i documenti e le comunicazioni di lavoro nei sistemi informativi messi a disposizione dall'Ente, evitando la conservazione esclusiva su dispositivi locali o archivi personali, al fine di garantirne la disponibilità in caso di assenza o cessazione del rapporto di lavoro.

9.3 Le modalità di accesso agli strumenti informatici e alle informazioni per esigenze organizzative o di sicurezza sono disciplinate da specifiche procedure interne adottate dall'Ente nel rispetto della normativa vigente.

10. Segnalazione di incidenti di sicurezza

10.1 Eventuali eventi che possano comportare rischi per la sicurezza delle informazioni o per la protezione dei dati personali devono essere tempestivamente segnalati al Referente in materia di protezione dei dati personali o al Responsabile della protezione dei dati (DPO), secondo le modalità previste dalla procedura interna per la gestione degli incidenti di sicurezza e delle violazioni di dati personali adottata dall'Ente.

11. Revisione e aggiornamento

11.1 Il presente documento potrà essere revisionato e aggiornato in relazione a mutamenti normativi o organizzativi dell'Ente.

12. Disposizioni finali

12.1 L'Ente provvede alla diffusione del presente documento con le modalità ritenute più opportune.