

**Segreteria**

Piazza del Municipio n. 6  
38024 COGOLO DI PEIO  
Tel 0463-754059  
Fax 0463-754465  
E-mail [c.peio@comuni.infotn.it](mailto:c.peio@comuni.infotn.it)

**COMUNE DI PEIO**Provincia di Trento

---

**ALLEGATO 1****Istruzioni e misure di sicurezza per il trattamento dei dati personali  
a cui si devono attenere gli incaricati**

Il presente documento, così come il Regolamento per l'accesso e l'utilizzo dei servizi internet e di posta elettronica comunale è da considerarsi parte integrante della nomina a incaricato del trattamento. Il contenuto del presente documento deve essere reso noto agli incaricati del trattamento, i quali sono tenuti a rispettarlo durante il periodo nel quale prestano attività lavorativa per il Comune di Peio.

**Segreteria**

Piazza del Municipio n. 6  
38024 COGOLO DI PEIO  
Tel 0463-754059  
Fax 0463-754465  
E-mail [c.peio@comuni.infn.it](mailto:c.peio@comuni.infn.it)

**COMUNE DI PEIO**

Provincia di Trento

**CONTENUTI**

<b>1</b>	<b>Finalità del presente documento .....</b>	<b>1</b>
<b>2</b>	<b>Definizioni.....</b>	<b>1</b>
<b>3</b>	<b>Norme nazionali vigenti e disposizioni dell'Ente che regolano il trattamento dei dati e l'utilizzo delle risorse informatiche comunali.....</b>	<b>2</b>
<b>4</b>	<b>Responsabilità .....</b>	<b>2</b>
4.1	Violazione della normativa italiana e del Regolamento Comunale sul trattamento dei dati personali .....	2
4.2	Segnalazione di violazioni delle istruzioni contenute nel presente documento.....	2
4.3	Procedimento disciplinare.....	2
4.4	Materiale Informativo .....	2
<b>5</b>	<b>Confidenzialità dei dati personali trattati .....</b>	<b>3</b>
<b>6</b>	<b>Precauzioni da adottare nel trattamento di dati personali contenuti in archivi e documenti cartacei .....</b>	<b>3</b>
6.1	Trattamento di documenti contenenti dati personali .....	3
6.2	Trattamento di documenti contenenti dati sensibili o giudiziari .....	3
6.3	Utilizzo di strumenti quali telefono, fax e scanner.....	3
<b>7</b>	<b>Precauzioni specifiche per gli incaricati addetti alla duplicazione di documentazione .....</b>	<b>4</b>
7.1	Cura nel disporre dei documenti originali .....	4
7.2	Distruzione delle copie cartacee non più occorrenti .....	4
<b>8</b>	<b>Precauzioni specifiche per i rapporti di Front-Office .....</b>	<b>4</b>
8.1	Rispetto della distanza di sicurezza.....	4
8.2	Identificazione dell'interessato .....	5
8.3	Diligenza nell'imputazione di dati.....	5
<b>9</b>	<b>Utilizzi consentiti del sistema informatico comunale.....</b>	<b>5</b>
9.1	Utilizzatori.....	5
9.2	Utilizzi consentiti .....	5
<b>10</b>	<b>Precauzioni da adottare per la tutela della sicurezza del sistema informatico comunale.....</b>	<b>5</b>
10.1	Regole generali riguardanti la sicurezza.....	5
10.2	Custodia della postazione di lavoro .....	6
10.3	Gestione delle password.....	6
10.4	Protezione dai virus .....	6
<b>11</b>	<b>Manutenzione e ottimizzazione delle risorse informatiche.....</b>	<b>7</b>
11.1	Custodia e manutenzione della postazione di lavoro .....	7



## Istruzioni e misure di sicurezza per il trattamento dei dati personali a cui si devono attenere gli incaricati

### 1 Finalità del presente documento

Le finalità di questo documento sono:

Stabilire le istruzioni operative e le misure di sicurezza a cui devono attenersi gli incaricati nel trattamento dei dati personali, con particolare attenzione al trattamento dei dati personali effettuati tramite strumenti informatici (ai sensi dell'art. 27 del disciplinare tecnico in materia di misure minime di sicurezza);

Assicurare che le risorse informatiche dell'Ente siano utilizzate esclusivamente per il raggiungimento delle finalità istituzionali;

Informare gli incaricati riguardo le norme nazionali vigenti e le disposizioni dell'Ente che regolano l'utilizzo delle risorse informatiche comunali.

### 2 Definizioni

Al fine di agevolare la comprensione delle istruzioni, in questa sezione vengono definiti i termini tecnici ricorrenti nel documento:

**Comunicazione elettronica:** qualsiasi comunicazione creata, inviata, inoltrata, trasmessa, archiviata, copiata, scaricata, mostrata, vista o stampata da uno o più sistemi o servizi di comunicazione elettronica.

**Policy o Regolamento:** documento che ha ad oggetto la regolazione di una determinata funzione dell'Ente. Può contenere delle linee guida e dei suggerimenti per una migliore fruizione dei servizi comunali.

**Responsabile del sistema informatico comunale:** persona responsabile della sicurezza e della gestione delle Risorse informatiche comunali.

**Risorse informatiche comunali:** qualsiasi combinazione di apparati tecnologici dell'Ente, hardware o software, utilizzati per le comunicazioni elettroniche ed elaborazione dei dati.

**Ufficio Sistema Informativo Comunale (SIC):** struttura organizzativa che - all'interno dell'Ente - si occupa della gestione operativa delle risorse informatiche comunali.

**Utente:** qualsiasi persona che accede alle Risorse informatiche comunali.



### **3 Norme nazionali vigenti e disposizioni dell'Ente che regolano il trattamento dei dati e l'utilizzo delle risorse informatiche comunali**

Per quanto concerne il trattamento dei dati personali e l'utilizzo delle risorse informatiche comunali, gli incaricati devono attenersi alle leggi, regolamenti e istruzioni elencati di seguito:

- Codice sulla protezione dei dati personali emanato con D.Lgs. 196/2003;
- Regolamento Comunale per il trattamento dei dati personali;
- Istruzioni e misure di sicurezza contenute nel presente documento;
- Ulteriori istruzioni impartite dal titolare o dai responsabili del trattamento dei dati personali
- Regolamento per l'accesso e l'utilizzo dei servizi Internet e di posta elettronica Comunali

### **4 Responsabilità**

#### **4.1 Violazione della normativa italiana e del Regolamento Comunale sul trattamento dei dati personali**

Qualsiasi violazione alla normativa italiana da parte degli utenti verrà segnalata alle autorità competenti. Il mancato rispetto o la violazione delle regole contenute nel presente regolamento è perseguibile con provvedimenti disciplinari nonché con le azioni civili e penali consentite.

#### **4.2 Segnalazione di violazioni delle istruzioni contenute nel presente documento**

Non sono ammesse segnalazioni di violazioni in forma anonima. Nei limiti previsti dalla normativa italiana, l'Ente tutela il diritto alla privacy degli utenti che comunicano dette violazioni.

#### **4.3 Procedimento disciplinare**

In caso di violazione delle istruzioni contenute nel presente documento, si applica il procedimento disciplinare previsto nel contratto di lavoro e negli accordi sindacali.

#### **4.4 Materiale Informativo**

Oltre al presente documento l'Ente potrà mettere a disposizione degli utenti del materiale informativo utile alla corretta implementazione della policy dell'Ente in materia di trattamento dei dati.



## **5 Confidenzialità dei dati personali trattati**

Gli incaricati sono tenuti a mantenere l'assoluta segretezza sulle informazioni di cui vengono a conoscenza nel corso delle operazioni di trattamento, evitando qualsiasi loro diffusione.

Gli incaricati sono tenuti a non parlare di questioni riservate in aree pubbliche (ad es.: ristoranti, aeroporti, mezzi di trasporto pubblico, newsgroup su Internet...) in modo tale che terzi possano udire la conversazione e a non mostrare, anche accidentalmente, documenti contenenti informazioni riservate.

## **6 Precauzioni da adottare nel trattamento di dati personali contenuti in archivi e documenti cartacei**

### **6.1 Trattamento di documenti contenenti dati personali**

Gli incaricati sono tenuti a custodire e controllare gli atti e i documenti contenenti dati personali, in modo da evitare che persone prive di autorizzazione possano accedere ai dati.

I documenti contenenti dati personali devono essere conservati in archivi ad accesso controllato e con possibilità di chiusura.

Tutta la documentazione e le pratiche trattate o da trattare devono essere riposte in armadi chiusi a chiave nel periodo di intervallo meridiano o al termine della giornata lavorativa.

### **6.2 Trattamento di documenti contenenti dati sensibili o giudiziari**

I documenti contenenti dati sensibili o giudiziari devono essere classificati come tali e resi riconoscibili agli altri incaricati ed in particolare al personale preposto all'archiviazione.

I documenti contenenti dati sensibili o giudiziari devono essere conservati in armadi chiusi.

### **6.3 Utilizzo di strumenti quali telefono, fax e scanner**

Nel caso di richieste di dati personali tramite fax l'incaricato deve prestare attenzione a:

- verificare l'identità del richiedente (ad esempio formulando una serie di quesiti a mezzo di intervista guidata oppure attribuendo all'interessato un codice identificativo che quest'ultimo gli comunicherà previamente ad ogni comunicazione impersonale);
- verificare, se necessario, che il dato richiesto sia stato riportato sul documento in modo corretto;
- digitare correttamente il numero di telefono del destinatario e controllarne l'esattezza prima dell'invio;
- verificare che il documento venga spedito correttamente;



- attendere la stampa del rapporto di trasmissione verificando la corrispondenza tra il numero di pagine da inviare e quelle effettivamente inviate.

Nel caso di richieste di dati personali tramite telefono è necessario prestare attenzione a:

- verificare l'identità del richiedente (ad esempio formulando una serie di quesiti a mezzo di intervista guidata oppure attribuendo all'interessato un codice identificativo che quest'ultimo gli comunicherà previamente ad ogni comunicazione impersonale).
- chiedere il numero di telefono dal quale è effettuata la chiamata.
- controllare che il dato richiesto sia stato comunicato all'interessato fedelmente.

Nel caso in cui gli incaricati procedano ad acquisire in formato digitale della documentazione cartacea tramite scanner devono verificare che il contenuto del documento oggetto di scansione sia correttamente leggibile.

## **7 Precauzioni specifiche per gli incaricati addetti alla duplicazione di documentazione**

### **7.1 Cura nel disporre dei documenti originali**

Gli incaricati preposti alla duplicazione di documentazione o alla sostituzione della documentazione cartacea con registrazione ottica devono prestare attenzione a non dimenticare l'originale del documento all'interno della macchina fotocopiatrice e/o dello scanner.

### **7.2 Distruzione delle copie cartacee non più occorrenti**

Gli incaricati preposti alla duplicazione di documentazione devono procedere alla distruzione controllata delle copie superflue, non più occorrenti o che presentino una forma non corretta. E' necessario che evitino di gettare la documentazione nel cestino della carta straccia senza aver previamente provveduto a rendere inintelligibili i dati impressi sul supporto.

## **8 Precauzioni specifiche per i rapporti di Front-Office**

### **8.1 Rispetto della distanza di sicurezza**

Gli operatori di sportello sono tenuti a richiedere il rispetto dello spazio di cortesia. Ove necessario, devono invitare gli interessati a sostare dietro le linee tracciate sul pavimento o dietro le barriere che delimitano lo spazio di riservatezza.



## **8.2 Identificazione dell'interessato**

Nei casi in cui sia necessario verificare l'identità dell'interessato per esigenze di garanzia di correttezza del dato da raccogliere, si suggerisce di richiedere ed ottenere un documento di riconoscimento.

## **8.3 Diligenza nell'imputazione di dati**

L'incaricato deve prestare attenzione in sede di inserimento dei dati personali dell'interessato al fine di evitare errori di battitura che potrebbero creare problemi nel proseguo del processo.

# **9 Utilizzi consentiti del sistema informatico comunale**

## **9.1 Utilizzatori**

L'uso delle risorse informatiche comunali è riservato ai dipendenti e ai collaboratori dell'Ente appositamente autorizzati.

Esse non possono quindi essere utilizzate da altre persone, salvo esplicita autorizzazione del Responsabile del sistema informatico comunale. Qualsiasi operazione effettuata tramite il codice identificativo e/o la password dell'utente sarà assegnata in termini di responsabilità all'utente assegnatario dei medesimi.

## **9.2 Utilizzi consentiti**

Le risorse informatiche sono di proprietà dell'Ente e devono essere utilizzate per il conseguimento dei suoi fini istituzionali. Non possono in alcun modo essere usate per scopi diversi.

Non vengono rilasciate copie o autorizzazioni di utilizzo di applicazioni o componenti software licenziati a nome dell'Ente per scopi privati.

# **10 Precauzioni da adottare per la tutela della sicurezza del sistema informatico comunale.**

## **10.1 Regole generali riguardanti la sicurezza**

Per qualsiasi dubbio riguardante la sicurezza informatica, gli utenti devono fare riferimento esclusivamente al Responsabile del sistema informatico comunale o persona da lui delegata.

In nessun caso l'utente comunica via e-mail, telefono, fax o altro mezzo di comunicazione non sicuro le proprie password o altre informazioni riservate inerenti al sistema informatico comunale.

Si raccomanda agli utenti di prestare la massima attenzione nella stampa di documenti contenenti dati personali, soprattutto nel caso si utilizzino delle stampanti di gruppo o accessibili a più persone.



Per nessuna ragione l'utente comunica a terzi le proprie password o altre informazioni riservate inerenti al sistema informatico comunale senza l'autorizzazione del Responsabile del sistema informatico comunale.

Qualsiasi persona delegata a coadiuvare il lavoro del Responsabile del sistema informatico comunale dovrà essere nominato in un apposito documento reso pubblico agli utenti dell'Ente.

Qualsiasi supporto informatico mobile che permetta di portare dati all'esterno dell'Ente rappresenta un grave rischio e un punto di vulnerabilità per la sicurezza del sistema informatico comunale. Questi supporti portatili non dispongono infatti di adeguati sistemi di sicurezza. La replica su questi strumenti di qualsiasi dato personale potrebbe fornire a terzi informazioni riservate in caso di smarrimento, furto o sequestro dell'apparecchio.

## **10.2 Custodia della postazione di lavoro**

Gli utenti sono tenuti a non lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento, anche in caso di temporaneo allontanamento dalla postazione di lavoro. L'utente potrà configurare il blocco preimpostato a tempo della propria postazione attraverso screen saver o in alternativa dovrà manualmente provvedere al blocco della postazione in caso di allontanamento anche temporaneo.

## **10.3 Gestione delle password**

Gli utenti sono tenuti a conservare la segretezza della propria password.

Gli utenti sono tenuti in ogni caso a sostituire la password ogni 6 mesi in caso di trattamento di dati personali comuni e ogni 3 mesi in caso di trattamento di dati sensibili o giudiziari.

Le password dovranno essere composte da almeno 8 caratteri alfanumerici.

Gli utenti sono tenuti a sostituire immediatamente la password, dandone comunicazione al Responsabile del sistema informatico comunale, nel caso si sospetti che la stessa abbia perso la segretezza.

Nel caso l'utente venisse a conoscenza delle password di altro utente, è tenuto a darne immediata notizia al Responsabile del sistema informatico comunale.

## **10.4 Protezione dai virus**

L'utente è tenuto a seguire attentamente le disposizioni date dall'Ufficio Sistema Informativo Comunale riguardo alla protezione da virus e da altri software pericolosi per il sistema informatico comunale.

Nel caso in cui il software antivirus rilevi la presenza di un virus, l'utente deve immediatamente: a) sospendere ogni elaborazione in corso senza spegnere il computer; b) segnalare l'accaduto all'Ufficio Sistema Informativo Comunale.

Non è consentito l'utilizzo di floppy disk, cd rom, cd riscrivibili e nastri magnetici di provenienza ignota.



Ogni dispositivo magnetico di provenienza esterna all'Ente deve essere verificato mediante il programma antivirus prima del suo utilizzo e, nel caso venga rilevato un virus, deve essere consegnato all'amministratore di sistema.

## **11 Manutenzione e ottimizzazione delle risorse informatiche**

### **11.1 Custodia e manutenzione della postazione di lavoro**

Ogni utente è responsabile dell'integrità e del buon funzionamento della propria postazione di lavoro, delle periferiche ad essa collegate e del software utilizzato. A questo proposito si raccomanda di spegnere a fine lavoro la propria postazione (unità di base e dispositivi periferici, quali stampanti, scanner, masterizzatori) come misura per prevenire possibili surriscaldamenti o eventi accidentali negli uffici, a norma del Decreto Legge 626/94 sulla Prevenzione infortuni Sicurezza ed Igiene negli ambienti di lavoro.

Non è permesso aggiungere, disinstallare o comunque modificare il software fornito o la configurazione della propria postazione; la violazione di tale regola non consente all'Ufficio Sistema informatico comunale di garantire il corretto funzionamento delle strumentazione informatica in dotazione agli uffici.

In tutti i casi in cui si rende necessario installare nuove postazioni di lavoro o dotare quelle già in essere di nuove componenti o programmi, la richiesta va sottoposta direttamente all'Ufficio Sistema informatico comunale, che ne valuterà la fattibilità, demandandone l'implementazione, se del caso, a risorse interne o mediante acquisizione/sviluppo di applicativi con società terze parti.



## **ALLEGATO 2**

### **Regolamento per l'accesso e l'utilizzo dei servizi internet e di posta elettronica comunali**

Il seguente documento, così come le istruzioni operative per il trattamento dei dati personali è da considerarsi parte integrante della nomina a incaricato del trattamento. Il contenuto del presente documento deve essere reso noto agli incaricati del trattamento, i quali sono tenuti a rispettarlo durante il periodo nel quale prestano attività lavorativa per il Comune di Peio.



<b>1</b>	<b>Finalità del presente documento</b> .....	<b>2</b>
<b>2</b>	<b>Definizioni</b> .....	<b>2</b>
<b>3</b>	<b>Norme nazionali vigenti e disposizioni dell'Ente che regolano il trattamento dei dati e l'utilizzo delle risorse informatiche comunali</b> .....	<b>2</b>
<b>4</b>	<b>Responsabilità</b> .....	<b>3</b>
4.1	Responsabilità nell'utilizzo dei servizi Internet e di posta elettronica Comunali.....	3
4.2	Procedimento disciplinare e indennità del Comune .....	4
4.3	Violazione della normativa italiana di settore .....	4
4.4	Materiale Informativo .....	4
<b>5</b>	<b>Disposizioni comuni all'accesso e all'utilizzo dei servizi Internet e di posta elettronica comunali</b>	<b>4</b>
5.1	Utilizzatori .....	4
5.2	Utilizzi consentiti dei servizi Internet e di posta elettronica comunali.....	4
5.3	Modalità di accesso ai servizi Internet e di posta elettronica comunali .....	5
<b>6</b>	<b>Misure da adottare per tutelare la sicurezza e la privacy nella navigazione in Internet</b> .....	<b>5</b>
6.1	Connessione ad Internet.....	5
6.2	Configurazione del Web Browser .....	5
6.3	Navigazione sicura.....	5
6.4	Rilascio di informazioni personali o dell'Ente durante la navigazione .....	6
6.5	Altri consigli per la navigazione in Internet .....	6
<b>7</b>	<b>Misure da adottare per tutelare la sicurezza e la privacy nell'utilizzo della posta elettronica</b> .....	<b>6</b>
7.1	Confidenzialità .....	6
7.2	Attendibilità del mittente.....	6
7.3	Gestione delle liste di destinatari.....	7
7.4	Contenuto dei messaggi .....	7
7.5	Altri consigli per l'utilizzo della posta elettronica.....	7
<b>8</b>	<b>Sistemi di risposta automatica, nomina del fiduciario e disclaimer in calce alle email</b> .....	<b>9</b>
8.1	Sistemi di risposta automatica .....	9
8.2	Nomina del fiduciario da parte del lavoratore .....	9
8.3	Disclaimer da porre in calce ai messaggi email del Comune.....	9
<b>9</b>	<b>Controlli del Comune sull'accesso e l'utilizzo dei servizi Internet e di Posta Elettronica tramite i PC comunali da parte degli utenti</b> .....	<b>1</b>
9.1	Registrazione delle attività sull'uso dei servizi.....	1
9.2	Principio di necessità dei controlli del Comune sull'uso degli strumenti elettronici, sull'accesso e l'utilizzo dei servizi Internet e di posta elettronica da parte degli utenti .....	1
9.3	Graduazione dei controlli .....	1
9.4	Facoltà di opposizione degli utenti al trattamento di dati personali contenuti nei log (art. 7 d.lgs 196/03) .....	1
<b>10</b>	<b>Cessazione d'ufficio dei servizi Internet e di posta elettronica comunali</b> .....	<b>2</b>



## 1 Finalità del presente documento

Il presente documento:

- disciplina l'accesso e l'utilizzo dei servizi Internet e di Posta Elettronica (email) Comunali da parte dei dipendenti e/o dei collaboratori comunali;
- detta linee guida da seguire per l'utilizzo sicuro dei servizi Internet e di Posta Elettronica (email) comunali
- definisce le modalità di controllo sull'utilizzo dei servizi Internet e di Posta Elettronica (email) Comunali da parte dei dipendenti e/o dei collaboratori comunali, sottolineando che tale controllo viene effettuato nel pieno rispetto dello Statuto dei lavoratori e degli accordi sindacali;
- specifica le sanzioni che il Comune può attuare in caso di mancato rispetto reiterato del presente Regolamento

## 2 Definizioni

**Internet Service Provider (ISP):** l'Azienda che fornisce al Comune di Peio la connettività alla rete Internet

**Log:** l'archivio delle attività di consultazione in rete

**Policy o Regolamento:** documento che ha ad oggetto la regolazione di una determinata funzione dell'Ente. Può contenere delle linee guida e dei suggerimenti per una migliore fruizione dei servizi comunali.

**Postazione di lavoro:** la macchina collegata alla rete comunale tramite la quale l'incaricato autorizzato accede ai servizi Internet e di posta elettronica (email).

**Responsabile del sistema informatico comunale:** persona responsabile della sicurezza e della gestione delle Risorse informatiche comunali.

**Risorse informatiche comunali:** qualsiasi combinazione di apparati tecnologici dell'Ente, hardware o software, utilizzati per le comunicazioni elettroniche ed elaborazione dei dati.

**Utente:** il dipendente e/o il collaboratore autorizzato dal Comune ad utilizzare le risorse informatiche comunali.

## 3 Norme nazionali vigenti e disposizioni dell'Ente che regolano il trattamento dei dati e l'utilizzo delle risorse informatiche comunali

Per quanto concerne l'utilizzo delle risorse informatiche comunali, gli incaricati devono attenersi alle leggi, regolamenti e istruzioni elencati di seguito:

- Codice sulla protezione dei dati personali emanato con D.Lgs. 196/2003;
- Istruzioni e misure di sicurezza a cui gli incaricati si devono attenere quando trattano dati personali;



- ulteriori eventuali istruzioni impartite dal titolare o dai responsabili del trattamento dei dati personali.

## **4 Responsabilità**

### **4.1 Responsabilità nell'utilizzo dei servizi Internet e di posta elettronica Comunali**

L'utente è direttamente e totalmente responsabile dell'uso che egli fa del servizio di accesso a Internet, dei contenuti che vi ricerca, dei siti che contatta, delle informazioni che vi immette e delle modalità con cui opera.

L'utente sarà pertanto civilmente responsabile di qualsiasi danno arrecato al Comune, all'Internet provider e/o a terzi in dipendenza della mancata osservanza di quanto previsto dal presente Regolamento.

L'utente si assume la responsabilità civile per i propri fatti illeciti e per quelli commessi da chiunque utilizzi il suo codice identificativo e/o password con particolare riferimento all'immissione in rete di contenuti critici o idonei a offendere l'ordine pubblico o il buon costume così come definiti dalla giurisprudenza della Corte di Cassazione.

Lo scarico di immagini, di file audio o musicali, di file video e in ogni caso di grandi quantità di dati in grado di degradare le prestazioni offerte dal servizio agli altri utenti può avvenire solo in casi eccezionali su espressa autorizzazione del Segretario comunale.

All'utente non è consentito:

- servirsi o dar modo ad altri di servirsi della stazione di accesso a Internet per attività non istituzionali, attività poste in essere in violazione del diritto d'autore o altri diritti tutelati dalla normativa vigente;
- scaricare software da Internet; eventuali necessità dovranno essere appositamente richieste all'amministratore di sistema che provvederà allo scaricamento del software (se del caso dopo che l'utente abbia confermato di aver ricevuto l'autorizzazione al "download" da parte del Dirigente di competenza);
- utilizzare tecniche di "mail spamming" cioè di invio massiccio di comunicazioni a liste di distribuzione extraaziendali o di azioni equivalenti;
- utilizzare il servizio di posta elettronica per inoltrare catene di S. Antonio, giochi, scherzi, barzellette e altre e - mails che non siano di lavoro;
- utilizzare Internet Provider diversi da quello scelto ufficialmente dal Comune di Peio e la connessione di stazioni di lavoro aziendali alle reti di detti provider con sistemi di connessione diversi (es. modem) da quello centralizzato;
- usare la rete in modo difforme da quanto previsto dal presente documento e dalle leggi penali, civili e amministrative in materia di disciplina dell'attività e dei servizi svolti sulla rete.



- inviare e-mails a una pluralità di utenti o a tutti gli utenti è consentito solo nel caso in cui il contenuto del messaggio sia effettivamente utile all'intero gruppo/i.

#### **4.2 Procedimento disciplinare e indennità del Comune**

In caso di violazione delle istruzioni contenute nel presente documento, si applica il procedimento disciplinare previsto nel contratto di lavoro e negli accordi sindacali.

L'utente si obbliga a tenere indenne il Comune da tutte le perdite, danni responsabilità, costi, oneri e spese, ivi comprese le eventuali spese legali, che dovessero essere subite o sostenute quali conseguenze di qualsiasi inadempimento da parte dell'utente agli obblighi e garanzie previste in questo articolo e comunque connesse alla immissione delle informazioni in internet anche in ipotesi di risarcimento danni pretesi da terzi a qualunque titolo.

#### **4.3 Violazione della normativa italiana di settore**

Qualsiasi violazione alla normativa italiana da parte degli utenti verrà segnalata alle autorità competenti.

#### **4.4 Materiale Informativo**

Oltre al presente documento l'Ente potrà mettere a disposizione degli utenti del materiale informativo utile alla corretta implementazione della policy dell'Ente in materia di trattamento dei dati.

### **5 Disposizioni comuni all'accesso e all'utilizzo dei servizi Internet e di posta elettronica comunali**

#### **5.1 Utilizzatori**

L'accesso ai servizi Internet e di posta elettronica comunali e il loro utilizzo sono riservati ai dipendenti e ai collaboratori dell'Ente appositamente autorizzati.

I servizi Internet e di posta elettronica comunali non possono quindi essere utilizzati da altre persone, salvo esplicita autorizzazione del Responsabile del sistema informatico comunale.

#### **5.2 Utilizzi consentiti dei servizi Internet e di posta elettronica comunali**

I servizi Internet e di posta elettronica comunali sono uno strumento di lavoro. I dipendenti e i collaboratori autorizzati ad accedere alla rete Internet e alla posta elettronica tramite i PC del Comune utilizzano dunque tali servizi solo per scopi professionali.



L'utente è tenuto a non utilizzare il servizio Internet comunale per collegarsi a caselle di posta elettronica personali consultabili da Internet (ad es. le caselle di hotmail.com, yahoo.it, libero.it etc..) durante l'orario di lavoro.

### **5.3 Modalità di accesso ai servizi Internet e di posta elettronica comunali**

Prima di accedere ai servizi l'utente fornisce i suoi dati e prende visione del presente Regolamento.

Dopo aver letto il presente Regolamento l'utente può collegarsi ad Internet e alla posta elettronica tramite il PC a lui assegnato dal Comune. Dopo aver acceso il PC inserendo il suo username e la sua password personali, l'utente accede ai servizi senza ulteriore formalità.

La configurazione dei servizi viene effettuata esclusivamente dall'amministratore di sistema. All'utente non è concesso modificare tale configurazione.

## **6 Misure da adottare per tutelare la sicurezza e la privacy nella navigazione in Internet**

### **6.1 Connessione ad Internet**

E' vietato connettersi autonomamente alla rete Internet con sistemi di dialup a numeri esterni all'Ente, salvo autorizzazione del Responsabile del Sistema Informativo Comunale.

### **6.2 Configurazione del Web Browser**

E' vietato modificare le impostazioni del Web Browser stabilite dal Responsabile del Sistema Informativo Comunale.

### **6.3 Navigazione sicura**

Fatto salvo il divieto a navigare per fini diversi da quelli professionali, si suggerisce di evitare la navigazione in siti caratterizzati da scarsa serietà e attendibilità.

Nel corso della navigazione l'utente è tenuto a leggere con attenzione qualsiasi finestra, pop up o avvertenza prima di proseguire nella navigazione e in particolare prima di accettare delle condizioni contrattuali o di aderire a delle iniziative online.

E' fatto divieto assoluto di scaricare programmi o contenuti multimediali senza la previa autorizzazione del Responsabile del Sistema Informativo.

E' opportuno segnalare che la navigazione in Internet è sottoposta ad un controllo automatico che vieta l'accesso a siti ritenuti inopportuni e tutto il traffico Internet viene regolarmente registrato.



#### **6.4 Rilascio di informazioni personali o dell'Ente durante la navigazione**

Gli utenti sono invitati a limitare il rilascio di informazioni personali durante la navigazione via Web.

Qualsiasi informazione comunale prima di essere comunicata via Web deve essere autorizzata dalla Dirigente responsabile.

Qualora il Dirigente autorizzi la comunicazione di dati sensibili o informazioni riservate via Web è necessario accertarsi che vi sia la protezione della comunicazione attraverso SSL. E' opportuno quindi lasciare abilitato l'avviso di accesso a pagine protette.

#### **6.5 Altri consigli per la navigazione in Internet**

Gli utenti sono invitati ad organizzare in modo ordinato la propria cartella dei siti Preferiti.

Si consiglia agli utenti di salvare sul proprio spazio disco in locale i file .pdf e .doc scaricati dalla rete prima di aprirli.

### **7 Misure da adottare per tutelare la sicurezza e la privacy nell'utilizzo della posta elettronica**

#### **7.1 Confidenzialità**

La confidenzialità della posta elettronica e della comunicazione attraverso il Web è limitata in quanto i messaggi, transitando nella rete pubblica di Internet, possono essere visionati da terzi non autorizzati. Il livello di confidenzialità di una e-mail si avvicina di più a quello di una cartolina piuttosto che a quello di una lettera. Per questa ragione è fatto divieto assoluto di comunicare informazioni classificate come riservate o dati sensibili attraverso l'e-mail o attraverso il Web se non esplicitamente autorizzati dal Dirigente responsabile del Servizio.

L'invio di comunicazioni elettroniche con informazioni personali riguardo al personale dell'Ente è sottoposta alla disciplina prevista dal Codice sulla protezione dei dati personali emanato con d.lgs. 196/2003 e leggi seguenti ed è previsto pertanto un diritto d'accesso ai dati da parte degli interessati, anche qualora questi ultimi non risultino tra i destinatari della comunicazione elettronica.

#### **7.2 Attendibilità del mittente**

L'attendibilità dell'identità del mittente, della data ed ora esatta è molto limitata nella comunicazione via e-mail. E' relativamente facile, infatti, camuffare il mittente di una e-mail. Si richiede pertanto, ogni qual volta sia necessaria la certezza dell'identità del mittente, di verificarla con mezzi appropriati.



### **7.3 Gestione delle liste di destinatari**

Gli utenti devono organizzare l'agenda del proprio programma di posta elettronica in modo che non vi possano essere degli errori nella selezione dei destinatari dei messaggi.

Nell'invio di messaggi elettronici a molteplici destinatari interni all'Ente gli utenti sono invitati a non utilizzare la funzione Copia Carbone Nascosta (CCN, anche chiamata Blind Carbon Copy -Bcc), che permette di occultare ai destinatari la lista degli altri destinatari del messaggio.

### **7.4 Contenuto dei messaggi**

Gli utenti devono assicurarsi che nei loro messaggi elettronici non siano inserite inconsapevolmente informazioni su User e Password utilizzate per accedere ad altre applicazioni. In particolare va usata la massima cautela nell'invio a mezzo posta elettronica di pagine internet che potrebbero contenere nell'indirizzo informazioni utili a risalire alla User/Password utilizzata.

Gli utenti sono invitati a nominare correttamente i nomi dei file allegati alle e-mail, specificando, nel caso si procedesse ad inviare documenti soggetti a modifiche e revisioni, la versione corrente del file con dei numeri progressivi.

E' esplicitamente vietato l'invio di messaggi in risposta a richieste di adesione a programmi di catene di e-mail, indipendentemente dalle finalità presunte.

Gli utenti sono invitati a prestare attenzione nell'utilizzo della funzione "Rispondi" e "Rispondi a tutti" nel caso il messaggio originario sia stato inviato ad un numero elevato di destinatari.

### **7.5 Altri consigli per l'utilizzo della posta elettronica**

Gli utenti sono invitati a leggere quotidianamente la posta elettronica e a rispondere in tempi ragionevoli alle e-mail ricevute.

Gli utenti sono invitati a scrivere i propri messaggi di posta elettronica in plain text (7-bit ASCII) qualora non si siano previamente accertati che il destinatario è provvisto di un client di posta in grado di supportare la lettura di altri formati.

Gli utenti sono tenuti sempre ad accertarsi che gli eventuali allegati dei propri messaggi non eccedano la dimensione massima di 5 Mb. Qualora si riscontrasse la necessità di allegare un file di dimensioni superiori è buona norma che il mittente si assicuri previamente con il destinatario sulla possibilità di ricevere un messaggio di tali dimensioni.

Gli utenti sono invitati ad inviare allegati nei formati suggeriti dal Ministero per l'Innovazione, che raccomanda l'uso di formati per lo scambio di informazioni "aperti" cioè liberamente interpretabili. L'utilizzo di file con estensioni poco comuni potrebbe comportare la cancellazione del messaggio da parte del destinatario; comunque è possibile utilizzare formati convenzionalmente accettati tra mittente e destinatario. Si faccia riferimento all'Ufficio Sistema Informativo per dubbi in merito.



Si consiglia agli utenti di selezionare l'opzione che permette di inviare i messaggi immediatamente. La funzione che permette di metterli in coda per un successivo invio è caratterizzata da un'alta percentuale di casi di mancato o ritardato invio.

Si invitano gli utenti che hanno selezionato l'opzione di completamento automatico dell'indirizzo di prestare molta attenzione nella selezione dei destinatari.

Gli utenti devono periodicamente cancellare o organizzare in opportune cartelle la posta già letta. Una quantità troppo elevata di e-mail nella cartella predefinita di arrivo della nuova posta può compromettere sensibilmente la stabilità del programma di posta.

Gli utenti devono sempre indicare con chiarezza (nel campo oggetto), l'argomento del proprio messaggio. E' possibile richiedere una ricevuta di corretto ricevimento della propria mail. A tale ricevuta va tuttavia assegnata una importanza relativa poiché talvolta la conferma della ricezione avviene ad opera del mail server centrale e non del destinatario ultimo del messaggio.

Gli utenti sono invitati a fare uso degli appositi filtri per l'organizzazione delle mail in arrivo ed in particolare per ridurre le perdite di tempo associate all'arrivo di messaggi di posta non sollecitati (spam).

Gli utenti sono invitati a segnalare all'Ufficio sistema Informativo comunale l'arrivo sistematico di messaggi non sollecitati (spam) da determinati indirizzi e-mail.

Gli utenti sono invitati ad utilizzare dei modelli di posta elettronica per i messaggi che vengono inviati frequentemente.

Gli utenti sono invitati a prestare la massima attenzione nell'utilizzo delle funzioni avanzate di filtro che consentono di inoltrare automaticamente determinati messaggi in arrivo ad altri destinatari.



## **8 Sistemi di risposta automatica, nomina del fiduciario e disclaimer in calce alle email**

### **8.1 Sistemi di risposta automatica**

Per prevenire l'apertura della posta elettronica dei dipendenti e per rispettare il principio di necessità e non eccedenza del trattamento di dati personali, Il Comune mette a disposizione di ciascun lavoratore apposite funzionalità di sistema che consentano di inviare automaticamente, in caso di assenze (ad es., per ferie o attività di lavoro fuori sede), messaggi di risposta contenenti le "coordinate" (anche elettroniche o telefoniche) di un altro soggetto o altre utili modalità di contatto della struttura.

Il dipendente è tenuto ad avvalersi di tali modalità appena esse sono state messe a disposizione dal Comune.

In caso di eventuali assenze non programmate (ad es., per malattia), qualora il lavoratore non possa attivare la procedura descritta (anche avvalendosi di servizi webmail), il titolare del trattamento, perdurando l'assenza oltre un determinato limite temporale, può disporre lecitamente, sempre che sia necessario e mediante personale appositamente incaricato (ad es., l'amministratore di sistema oppure, se presente, un incaricato aziendale per la protezione dei dati), l'attivazione di un analogo accorgimento, avvertendo gli interessati.

### **8.2 Nomina del fiduciario da parte del lavoratore**

In previsione della 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 di un dipendente, l'interessato è messo in grado di delegare un altro lavoratore (fiduciario) a:

- verificare il contenuto di messaggi e a
- inoltrare al titolare del trattamento quelli ritenuti rilevanti per lo svolgimento dell'attività lavorativa.

A cura del Titolare del trattamento, di tale attività dovrebbe essere redatto apposito verbale e informato il lavoratore interessato alla prima occasione utile.

### **8.3 Disclaimer da porre in calce ai messaggi email del Comune**

I messaggi di posta elettronica inviati tramite il sistema di posta elettronica comunale devono contenere un avvertimento ai destinatari, nel quale viene dichiarata l'eventuale natura non personale dei messaggi stessi, precisando se le risposte potranno essere conosciute nell'organizzazione di appartenenza del mittente.



## **9 Controlli del Comune sull'accesso e l'utilizzo dei servizi Internet e di Posta Elettronica tramite i PC comunali da parte degli utenti**

### **9.1 Registrazione delle attività sull'uso dei servizi**

Le attività sull'uso dei servizi Internet e di posta elettronica dell'utente vengono registrate elettronicamente sotto forma di file di log.

L'attività di registrazione viene effettuata a cura dell'amministratore di sistema, che garantisce anche la custodia dei file di log.

### **9.2 Principio di necessità dei controlli del Comune sull'uso degli strumenti elettronici, sull'accesso e l'utilizzo dei servizi Internet e di posta elettronica da parte degli utenti**

Nel rispetto del divieto di controllo a distanza del lavoratore e dello Statuto dei Lavoratori nel quale tale divieto è contenuto, il Comune effettua controlli sull'uso degli strumenti elettronici da parte degli utenti tramite consultazione dei file di log solo in relazione:

- ad esigenze di sicurezza del tutto particolari (ad es. nel caso in cui l'integrità del sistema sia minata da un problema di sicurezza e sia necessaria la consultazione dei file di log per individuare e eliminare l'anomalia);
- all'indispensabilità dei dati di log rispetto all'esercizio o alla difesa di un diritto in sede giudiziaria;
- all'obbligo di rispondere ad una specifica richiesta dell'autorità giudiziaria o della polizia giudiziaria.

Le stesse esigenze sono necessarie per motivare un prolungamento della conservazione dei log rispetto al normale termine di conservazione.

### **9.3 Graduazione dei controlli**

Nel caso in cui sia necessaria l'analisi del contenuto dei file di log per esigenze di sicurezza particolari (9.1), il Comune effettua un controllo preliminare su dati aggregati (riferiti all'intera struttura lavorativa o a una sua area). Solo se l'analisi sui dati aggregati non risulta idonea alla soluzione del problema di sicurezza il Comune procede ad un'analisi che preveda il trattamento dei dati personali dell'utente.

### **9.4 Facoltà di opposizione degli utenti al trattamento di dati personali contenuti nei log (art. 7 d.lgs 196/03)**

Gli utenti hanno facoltà opporsi ai trattamenti effettuati nei casi menzionati in 9.1 per motivi legittimi.



## 10 Cessazione d'ufficio dei servizi Internet e di posta elettronica comunali

Ai sensi della presente informativa, l'utilizzo del servizio di accesso ad internet cesserà d'ufficio nei seguenti casi:

- qualora non sussistesse più la condizione di dipendente o collaboratore autorizzato o non fosse confermata l'autorizzazione all'uso;
- qualora venga accertato un uso non corretto del servizio da parte dell'utente o comunque un uso estraneo ai suoi compiti professionali;
- qualora vengano sospettate manomissioni e/o interventi sul hardware e/o sul software dell'utente impiegati per la connessione compiuti eventualmente da personale non autorizzato;
- in caso di diffusione o comunicazione imputabili direttamente o indirettamente all'utente, di password, procedure di connessione, indirizzo I.P. ed altre informazioni tecniche riservate;
- in caso di accesso doloso dell'utente a directory, a siti e/o file e/o servizi da chiunque resi disponibili non rientranti fra quelli per lui autorizzati e in ogni caso qualora l'attività dell'utente comporti danno, anche solo potenziale al sito contattato;
- in caso di concessione di accesso ad internet diretta o indiretta a qualsiasi titolo da parte dell'utente a terzi;
- in caso di violazione e/o inadempimento imputabile all'utente di quanto stabilito nel presente Regolamento

Il Comune si riserva la facoltà di sospendere a propria discrezione l'accesso al servizio qualora sussistano ragionevoli evidenze di una violazione degli obblighi dell'utente.

