



# CITTA' DI CIVIDALE DEL FRIULI

I-33043 – Corso Paolino d'Aquileia, 2 – ☎ 0432.710100, 📠 0432.710103  
e-mail: [comune.cividaledelfriuli@CERTgov.fvg.it](mailto:comune.cividaledelfriuli@CERTgov.fvg.it), sito internet: [www.comune.cividale-del-friuli.ud.it](http://www.comune.cividale-del-friuli.ud.it)

## **REGOLAMENTO PER L'UTILIZZO DEGLI STRUMENTI INFORMATICI**

**Approvato con Deliberazione G.M. n. 30 del 28 gennaio 2019**

## Indice

<b>INDICE</b> .....	<b>1</b>
<b>CHANGELOG – REGISTRO DELLE MODIFICHE</b> .....	<b>3</b>
<b>1 - OGGETTO E FINALITÀ</b> .....	<b>4</b>
<b>2 - PRINCIPI GENERALI E DI RISERVATEZZA NELLE COMUNICAZIONI</b> .....	<b>5</b>
<b>3 - TUTELA DEL LAVORATORE</b> .....	<b>6</b>
<b>4 - CAMPO DI APPLICAZIONE</b> .....	<b>6</b>
<b>5 - GESTIONE, ASSEGNAZIONE E REVOCA DELLE CREDENZIALI DI ACCESSO</b> .....	<b>6</b>
<b>6 - UTILIZZO DELLA RETE DEL COMUNE DI CIVIDALE DEL FRIULI</b> .....	<b>7</b>
<b>7 - UTILIZZO DEGLI STRUMENTI ELETTRONICI (PC, NOTEBOOK E ALTRI STRUMENTI CON RELATIVI SOFTWARE E APPLICATIVI)</b> .....	<b>8</b>
<b>8 - UTILIZZO DI INTERNET</b> .....	<b>11</b>
<b>9 - UTILIZZO DELLA POSTA ELETTRONICA</b> .....	<b>13</b>
<b>10 - UTILIZZO DEI TELEFONI, FAX, FOTOCOPIATRICI, SCANNER E STAMPANTI DELL'ENTE</b> .....	<b>15</b>
<b>11 - ASSISTENZA AGLI UTENTI E MANUTENZIONI</b> .....	<b>17</b>
<b>12 - CONTROLLI SUGLI STRUMENTI (ART. 6.1 PROVV. GARANTE, AD INTEGRAZIONE DELL'INFORMATIVA EX ART. 13 D.LGS 196/03)</b> .....	<b>18</b>
<b>13 - CONSERVAZIONE DEI DATI</b> .....	<b>20</b>
<b>14 - PARTECIPAZIONE AI SOCIAL MEDIA</b> .....	<b>20</b>
<b>15 - ATTIVITA' SINDACALI E R.S.U.</b> .....	<b>20</b>
<b>16 - SANZIONI DISCIPLINARI</b> .....	<b>20</b>
<b>17 - ENTRATA IN VIGORE</b> .....	<b>20</b>
<b>18 - DIVULGAZIONE</b> .....	<b>20</b>

**Changelog – Registro delle modifiche**

Versione	Data	Cambiamenti effettuati dall'ultima versione
1.0	11.09.2018	DPO Paolo Vicenzotto / Gianfranco Mauri

## **Premessa**

Il presente Regolamento intende fornire ai dipendenti e collaboratori, denominati anche incaricati o utenti, del Comune di Cividale del Friuli le indicazioni per una corretta e adeguata gestione delle informazioni personali, in particolare attraverso l'uso di sistemi, applicazioni e strumenti informatici dell'Ente.

Si specifica che tutti gli strumenti utilizzati dal lavoratore, intendo con ciò i PC, notebook, risorse, e-mail ed altri strumenti con relativi software e applicativi (di seguito più semplicemente "Strumenti"), sono messi a disposizione dall'Ente per rendere la prestazione lavorativa. Gli Strumenti, nonché le relative reti dell'Ente a cui è possibile accedere tramite gli stessi, sono domicilio informatico del Comune di Cividale del Friuli.

I dati personali e le altre informazioni dell'Utente che sono registrati negli Strumenti o che si possono eventualmente raccogliere tramite il loro uso, sono utilizzati per finalità istituzionali, per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio dell'Ente. Per tutela del patrimonio dell'Ente si intende altresì la sicurezza informatica e la tutela del sistema informatico dell'Ente. Tali informazioni sono altresì utilizzabili a tutti i fini connessi al rapporto di lavoro, visto che il presente Regolamento costituisce adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli, sempre nel rispetto di quanto disposto dal Regolamento Europeo 679/2016 sulla protezione dei dati personali, come recepito con Decreto Legislativo n. 101 in data 10 agosto 2018.

Viene, infine, precisato che non sono installati o configurati sui sistemi informatici in uso agli utenti apparati hardware o strumenti software aventi come scopo il controllo a distanza dell'attività dei lavoratori.

## **1 - Oggetto e finalità**

Il presente Regolamento è redatto:

- alla luce della Legge 20.5.1970, n. 300, recante "Norme sulla tutela della libertà e dignità dei lavoratori, della libertà sindacale e dell'attività sindacale nei luoghi di lavoro e norme sul collocamento";
- in attuazione del Regolamento Europeo 679/2016 sulla protezione dei dati personali (d'ora in avanti Reg. 679/2016 o GDPR), come recepito con Decreto Legislativo n. 101 in data 10 agosto 2018;
- ai sensi delle "Linee guida del Garante per posta elettronica e internet" in Gazzetta Ufficiale n. 58 del 10 marzo 2007;
- alla luce dell'articolo 23 del D.Lgs. n. 151/2015 (c.d. Jobs Act) che modifica e rimodula la fattispecie integrante il divieto dei controlli a distanza, nella consapevolezza di dover tener conto, nell'attuale contesto produttivo, oltre agli impianti audiovisivi, anche degli altri strumenti «*dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori*» e di quelli «*utilizzati dal lavoratore per rendere la prestazione lavorativa*».

La finalità è quella di promuovere in tutto il personale dell'Ente una corretta "cultura informatica" affinché l'utilizzo degli Strumenti informatici e telematici forniti dall'Ente, quali la posta elettronica, internet e i personal computer con i relativi software, sia conforme alle finalità dell'Ente e pienamente rispettoso della legge. Si vuole fornire a tutto il personale le indicazioni necessarie con l'obiettivo principale di evitare il verificarsi di qualsiasi abuso o uso non conforme, muovendo dalla convinzione che la prevenzione dei problemi sia preferibile rispetto alla loro successiva correzione.

## 2 - Principi generali e di riservatezza nelle comunicazioni

2.1 I principi che sono a fondamento del presente Regolamento sono gli stessi espressi nel GDPR, e, precisamente:

- a) **il principio di necessità**, secondo cui i sistemi informativi e i programmi informatici devono essere configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi in relazione alle finalità perseguite (art. 5 e 6 del Reg. 679/2016);
- b) **il principio di correttezza**, secondo cui le caratteristiche essenziali dei trattamenti devono essere rese note ai lavoratori. Le tecnologie dell'informazione (in modo più marcato rispetto ad apparecchiature tradizionali) permettono di svolgere trattamenti ulteriori rispetto a quelli connessi ordinariamente all'attività lavorativa. Ciò, all'insaputa o senza la piena consapevolezza dei lavoratori, considerate anche le potenziali applicazioni di regola non adeguatamente conosciute dagli interessati;
- c) **i trattamenti devono essere effettuati per finalità determinate, esplicite e legittime** (art.5 commi 1 e 2), osservando il principio di pertinenza e non eccedenza. Il datore di lavoro deve trattare i dati "nella misura meno invasiva possibile"; le attività di monitoraggio devono essere svolte solo da soggetti preposti ed essere "mirate sull'area di rischio, tenendo conto della normativa sulla protezione dei dati e, se pertinente, del principio di segretezza della corrispondenza".

2.2 Il dipendente si attiene alle seguenti regole di trattamento:

- a) È vietato comunicare a soggetti non specificatamente autorizzati i dati personali comuni, sensibili, giudiziari, sanitari o altri dati, elementi e informazioni dell'Ente dei quali il dipendente / collaboratore viene a conoscenza nell'esercizio delle proprie funzioni e mansioni all'interno dell'Ente. In caso di dubbio, è necessario accertarsi che il soggetto cui devono essere comunicati i dati sia o meno autorizzato a riceverli, mediante richiesta preventiva al proprio Responsabile di area/funzione.
- b) È vietata l'estrazione di originali e/o copie cartacee ed informatiche per uso personale di documenti, manuali, fascicoli, lettere, data base e quant'altro.
- c) È vietato lasciare incustoditi documenti, lettere, fascicoli, appunti e quant'altro possa contenere dati personali e/o informazioni dell'Ente quando il dipendente/collaboratore si allontana dalla postazione di lavoro. È vietato lasciare sulla postazione di lavoro (scrivania, bancone ecc.) materiali che non siano inerenti la pratica che si sta trattando in quel momento. Ciò vale soprattutto nel caso di lavoratori con mansioni di front office.
- d) È vietato divulgare a familiari ed amici dettagli dell'attività svolta e della struttura informatica comunale.
- e) È vietato colloquiare con colleghi di attività d'ufficio, al telefono o di persona, in presenza di estranei.
- f) È vietato gettare atti e/o appunti d'ufficio nella spazzatura, se non dopo averli debitamente parcellizzati.
- g) Per le riunioni e gli incontri con utenti, cittadini, clienti, fornitori, consulenti e collaboratori dell'Ente è necessario utilizzare le apposite Sale dedicate.
- h) Moderare il tono della voce ogni qualvolta si trattino argomenti inerenti dati personali.
- i) Chiudere a chiave tutti i cassetti, gli armadi e le porte, al termine dei propri orari di servizio (nei locali muniti di più livelli di sicurezza – ad esempio armadio con serratura in stanza dotata di porta chiudibile con serratura – sarà sufficiente la chiusura a chiave di almeno un livello: ad esempio

chiusura della porta dell'ufficio per interdire l'accesso completo alla stanza oppure, in presenza di porta non chiudibile, la chiusura di ogni singolo armadio o cassetto).

### **3 - Tutela del lavoratore**

- 3.1 Alla luce dell'art. 4, comma 1, L.n. 300/1970, la regolamentazione della materia indicata nell'art. 1 del presente Regolamento, non è finalizzata all'esercizio di un controllo a distanza dei lavoratori da parte del datore di lavoro ma solo a permettere a quest'ultimo di utilizzare sistemi informativi per fare fronte ad esigenze produttive od organizzative e di sicurezza nel trattamento dei dati personali.
- 3.2 È garantito al singolo lavoratore il controllo sui propri dati personali secondo quanto previsto dagli articoli 15-16-17-18-20-21-78 del Reg. 679/2016.

### **4 - Campo di applicazione**

- 4.1 Il presente regolamento si applica a tutti i dipendenti, senza distinzione di ruolo e/o di livello, nonché a tutti i collaboratori dell'Ente a prescindere dal rapporto contrattuale con la stessa intrattenuto.
- 4.2 Ai fini delle disposizioni dettate per l'utilizzo delle risorse informatiche e telematiche, per "utente" deve intendersi ogni dipendente e collaboratore in possesso di specifiche credenziali di autenticazione. Tale figura potrà anche venir indicata come "incaricato del trattamento".

### **5 - Gestione, assegnazione e revoca delle credenziali di accesso**

- 5.1 Le credenziali di autenticazione per l'accesso alle risorse informatiche vengono assegnate dall'Ufficio Sistema Informativo Comunale, previa formale richiesta del Responsabile dell'Unità Operativa nell'ambito del quale verrà inserito ed andrà ad operare il nuovo utente. Nel caso di collaboratori esterni la richiesta dovrà essere inoltrata direttamente dal Responsabile dell'Unità Operativa con il quale il collaboratore si coordina nell'espletamento del proprio incarico. La richiesta di attivazione delle credenziali dovrà essere completa di generalità dell'utente ed elenco dei sistemi informativi per i quali deve essere abilitato l'accesso. Ogni successiva variazione delle abilitazioni di accesso ai sistemi informativi dovrà essere richiesta formalmente all'Ufficio Sistema Informativo Comunale dal Responsabile di riferimento.
- 5.2 Le credenziali di autenticazioni consistono in un codice per l'identificazione dell'utente (altresì nominati username, nome utente o user-id), assegnato dall'Ufficio Sistema Informativo Comunale, ed una relativa password. La password è personale e riservata e dovrà essere conservata e custodita dall'incaricato con la massima diligenza e non divulgata.
- 5.3 La password deve essere di adeguata robustezza: deve essere composta da almeno 8 caratteri, formata da lettere maiuscole e minuscole e/o numeri. Non deve contenere riferimenti agevolmente riconducibili all'utente (username, nomi o date relative alla persona o ad un familiare). Le password utilizzate per l'accesso ai diversi servizi devono essere diversificate, al fine di evitare la loro facile replicabilità.
- 5.4 È necessario procedere alla modifica della password a cura dell'utente al primo accesso e, successivamente, almeno ogni sei mesi. Nel caso in cui l'utente svolga mansioni che, in astratto, possano comportare il trattamento di dati personali sensibili, è obbligatorio il cambio password almeno ogni tre mesi.

- 5.5 Nel caso di cessazione del rapporto di lavoro con il dipendente/collaboratore, il Responsabile dell'Unità Operativa di riferimento dovrà comunicare formalmente e preventivamente all'Ufficio Sistema Informativo Comunale la data effettiva a partire dalla quale le credenziali saranno disabilitate. Qualora la cessazione del rapporto si riferisca al Responsabile dell'Unità Operativa stessa, spetta all'Ufficio Personale provvedere all'espletamento di tale incombenza.
- 5.6 Le credenziali d'accesso sono personali, segrete, non cedibili e non divulgabili. Ove tali codici d'accesso non siano stati attribuiti è vietato l'utilizzo di codici assegnati ad altri utenti.
- 5.7 Ogni utente deve conservare diligentemente tutte le credenziali d'accesso assegnate, in modo da consentire il loro facile e immediato recupero ed aggiornamento, garantendo nel contempo la riservatezza assoluta di tali informazioni. In caso di cessazione dal servizio, indipendentemente dalla motivazione (pensionamento, mobilità, trasferimento, ecc.) l'utente che dispone di credenziali relative ad account attivati in nome e per conto dell'Ente, dovrà procedere per tempo al relativo passaggio di consegne.

## **6 - Utilizzo della rete del Comune di Cividale del Friuli**

- 6.1 Per l'accesso alle risorse informatiche del Comune di Cividale del Friuli attraverso la rete locale, ciascun utente deve essere in possesso di proprie credenziali di autenticazione secondo l'art. 5.
- 6.2 È proibito accedere alla rete e nei sistemi informativi utilizzando credenziali di altre persone.
- 6.3 L'accesso alla rete garantisce all'utente la disponibilità di condivisioni di rete (cartelle su server) nelle quali vanno inseriti e salvati i files di lavoro, organizzati per Unità Operativa o per diversi criteri o per obiettivi specifici di lavoro. Ciascun utente, poi, dispone di un'area riservata e personale. Tutte le cartelle di rete, siano esse condivise o personali, possono ospitare esclusivamente contenuti professionali. Pertanto è vietato il salvataggio sui server dell'Ente, ovvero sugli Strumenti, di documenti non inerenti l'attività lavorativa, quali a titolo esemplificativo documenti, fotografie, video, musica, pratiche personali, sms, mail personali, film e quant'altro. Ogni materiale personale rilevato dall'Amministratore di Sistema a seguito di interventi di sicurezza informatica ovvero di manutenzione/aggiornamento su server ed anche su Strumenti viene rimosso secondo le regole previste nel successivo punto 12 del presente Regolamento, ferma ogni ulteriore responsabilità civile, penale e disciplinare. Tutte le risorse di memorizzazione, diverse da quelle citate al punto precedente, non sono sottoposte al controllo regolare dell'Amministratore di Sistema e non sono oggetto di backup periodici. A titolo di esempio e non esaustivo si citano: il disco C:\ o altri dischi locali dei singoli PC, la cartella "Documenti" o "Desktop" dell'utente, gli eventuali dispositivi di memorizzazione locali o di disponibilità personale come Hard disk portatili o NAS ad uso esclusivo. Tutte queste aree di memorizzazione non devono ospitare dati di interesse dell'Ente, poiché non sono garantite la sicurezza e la protezione contro la eventuale perdita di dati. Pertanto la responsabilità dei salvataggi dei dati ivi contenuti è a carico del singolo utente.
- 6.4 Senza il consenso del Responsabile della Unità Operativa, è vietato trasferire documenti elettronici dai sistemi informativi e Strumenti dell'Ente a device esterni (hard disk, chiavette, CD, DVD e altri supporti).
- 6.5 Senza il consenso dell'Ufficio Sistema Informativo Comunale è vietato salvare documenti elettronici dell'Ente (ad esempio pervenuti via mail o salvati sul Server o sullo Strumento in dotazione) su repository esterne (quali ad esempio Dropbox,

GoogleDrive, OneDrive, ecc.) ovvero inviandoli a terzi via posta elettronica o con altri sistemi.

- 6.6 Con regolare periodicità (almeno una volta al mese), ciascun utente provvede alla pulizia degli archivi (anche della posta elettronica), con cancellazione dei file obsoleti o inutili. Particolare attenzione deve essere prestata alla duplicazione dei dati, essendo infatti necessario evitare un'archiviazione ridondante.
- 6.7 il Comune di Cividale del Friuli mette a disposizione dei propri utenti la possibilità di accedere alle proprie risorse informatiche anche dall'esterno dei confini dell'Ente, mediante rete VPN (Virtual Private Network), un canale privato e criptato verso la rete interna. L'accesso mediante VPN viene concesso a consulenti, professionisti, tecnici e fornitori che nell'ambito di un rapporto contrattuale con il Comune di Cividale del Friuli necessitino di accedere a determinate risorse informatiche. Viene concesso, altresì, a dipendenti e funzionari del Comune di Cividale del Friuli che necessitino di svolgere compiti specifici, pur non essendo presenti in sede. Le richieste di abilitazione all'accesso mediante VPN dovranno seguire le prescrizioni del punto 5.
- 6.8 All'interno delle sedi del Comune di Cividale del Friuli è resa disponibile anche una rete senza fili, c.d. "Wi-Fi". Tali reti consentono l'accesso alle risorse dell'Ente e ad internet per i dispositivi non connessi alla rete LAN mediante cavo. L'accesso mediante rete Wi-Fi viene concesso a consulenti, professionisti, tecnici e fornitori che nell'ambito di un rapporto contrattuale con il Comune di Cividale del Friuli necessitino di accedere a determinate risorse informatiche. Viene concesso, altresì, a dipendenti e funzionari del Comune di Cividale del Friuli che necessitino di svolgere compiti specifici che non possono essere svolti dalle postazioni fisse. L'autorizzazione alla connessione Wi-Fi sarà rilasciata dall'Ufficio Sistema Informativo Comunale.
- 6.9 L'Ufficio Sistema informativo Comunale si riserva la facoltà di negare o interrompere l'accesso alla rete mediante dispositivi non adeguatamente protetti e/o aggiornati, che possano costituire una concreta minaccia per la sicurezza informatica dell'Ente.
- 6.10 Ove non esistano specifiche diverse disposizioni, è vietato inserire codici di protezione all'accesso su singoli files (ad esempio di elaborati con sistemi di trattamento testi, fogli di calcolo, ecc.).

I log relativi all'uso del File System e della intranet dell'Ente, nonché i file salvati o trattati su Server o Strumenti, sono registrati e possono essere oggetto di controllo da parte del Titolare del trattamento, attraverso l'Ufficio Sistema Informativo Comunale, per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio dell'Ente.

I controlli possono avvenire secondo le disposizioni previste al successivo punto 12 del presente Regolamento.

Le informazioni così raccolte sono altresì utilizzabili a tutti i fini connessi al rapporto di lavoro, compresa la verifica del rispetto del presente Regolamento, che costituisce adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli ai sensi del Regolamento Europeo 679/16 "General Data Protection".

## **7 - Utilizzo degli Strumenti elettronici (PC, notebook e altri strumenti con relativi software e applicativi)**

- 7.1 Il dipendente/collaboratore è consapevole che gli Strumenti forniti sono di proprietà del Comune di Cividale del Friuli e devono essere utilizzati esclusivamente per rendere la prestazione lavorativa. Ognuno è responsabile dell'utilizzo delle dotazioni



informatiche ricevute in assegnazione. Ogni utilizzo non inerente all'attività lavorativa è vietato in quanto può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza. Ciascun dipendente/collaboratore si deve quindi attenere alle seguenti regole di utilizzo degli Strumenti.

- 7.2 L'accesso agli Strumenti dell'Ente è protetto da password; per l'accesso devono essere utilizzati Username e password assegnate dall'Ufficio Sistema Informativo Comunale (cfr. 5). A tal proposito si rammenta che essi sono strettamente personali e l'utente è tenuto a conservarli nella massima segretezza.
- 7.3 Il Personal Computer, notebook, tablet ed ogni altro hardware deve essere custodito con cura da parte degli assegnatari evitando ogni possibile forma di danneggiamento e segnalando tempestivamente al personale dell'Ufficio Sistema Informativo Comunale ogni malfunzionamento e/o danneggiamento. Non è consentita l'attivazione della password d'accensione (BIOS), senza preventiva autorizzazione da parte dell'Amministratore di Sistema.
- 7.4 Non è consentito all'utente modificare le caratteristiche hardware e software impostate sugli Strumenti assegnati, salvo preventiva autorizzazione da parte dell'Amministratore di Sistema.
- 7.5 L'installazione di software sui posti-lavoro informatizzati può avvenire solamente a fronte di autorizzazione del Responsabile dell'Unità Operativa, previo nulla osta da parte del Sistema Informativo Comunale, con intervento di un Amministratore di sistema abilitato: tutti gli estremi delle licenze d'uso dei software installati, devono essere comunicati al Sistema Informativo Comunale.
- 7.6 I sistemi devono essere sempre custoditi: l'utente è tenuto a disattivare il sistema, o bloccarne l'accesso, ogni qualvolta sia costretto ad assentarsi dal locale nel quale è ubicato o nel caso ritenga di non essere in grado di presidiare l'accesso alla medesima: lasciare un PC incustodito connesso alla rete può essere causa di utilizzo da parte di terzi senza che vi sia la possibilità di provarne in seguito l'indebito uso.
- 7.7 I sistemi assegnati dovranno essere disattivati e spenti nella pausa meridiana ed al termine dell'orario di servizio.
- 7.8 I posti-lavoro informatizzati non possono essere resi inaccessibili localmente con sistemi di tipo fisico (hardware), al fine di permetterne la costante accessibilità da parte dell'assistenza tecnica e la loro pronta configurabilità e riallocazione fisica, per esigenze organizzative.
- 7.9 Le informazioni archiviate sui dispositivi informatici assegnati devono essere esclusivamente quelle necessarie all'attività lavorativa assegnata.
- 7.10 Costituisce buona regola la pulizia periodica (almeno mensile) degli archivi memorizzati sui sistemi in uso (PC, web-mail, ecc.), con cancellazione dei file obsoleti o non più utili.
- 7.11 La gestione dei dati sulle postazioni informatiche è demandata all'utente utilizzatore che dovrà provvedere a memorizzarli sulle condivisioni dell'Ente, in modo che i dati possano essere utilizzati anche da altri utenti, evitando sempre l'esclusività su di essi. Non è consentita l'installazione di programmi diversi da quelli autorizzati dall'Ufficio Sistema Informativo Comunale.
- 7.12 Gli operatori dell'Ufficio Sistema Informativo Comunale possono in qualunque momento procedere alla rimozione di ogni file o applicazione che riterranno essere pericolosi per la sicurezza dei PC, della rete locale e dei server dell'Ente, nonché tutte le impostazioni eventualmente configurate che possano interferire con il corretto funzionamento dei servizi informatici dell'Ente.

- 7.13 È obbligatorio consentire l'installazione degli aggiornamenti di sistema che vengono proposti automaticamente, al primo momento disponibile, in modo tale da mantenere il PC sempre protetto.
- 7.14 È vietato utilizzare il PC per l'acquisizione, la duplicazione e/o la trasmissione illegale di opere protette da copyright.
- 7.15 È vietato l'utilizzo di supporti di memoria magneto-ottici (chiavi USB, CD, DVD o altri supporti) per il salvataggio di dati trattati tramite gli Strumenti dell'Ente, salvo che il supporto utilizzato sia stato autorizzato dall'Amministratore di Sistema. In tale caso, il supporto fornito può essere utilizzato esclusivamente per finalità istituzionali dell'Ente.
- 7.16 È vietato connettere al PC qualsiasi periferica non autorizzata preventivamente dall'Amministratore di Sistema.
- 7.17 È vietato connettere alla rete locale qualsiasi dispositivo (PC esterni, router, switch, modem, etc.) non autorizzato preventivamente dall'Amministratore di Sistema, come è assolutamente vietato connettere alla rete comunale eventuali apparati personali di qualsiasi natura essi siano.
- 7.18 Nel caso in cui l'utente dovesse notare comportamenti anomali del PC, l'utente stesso è tenuto a comunicarlo tempestivamente all'Ufficio Sistema Informativo Comunale.
- 7.19 I sistemi messi a disposizione di utenti non sottoposti alle presenti prescrizioni (postazioni informatiche pubbliche presso la Biblioteca, l'Informacittà, ecc.), non possono accedere alla rete del Sistema Informativo Comunale. Saranno pertanto instradati su apposite distinte reti virtuali ed avranno accesso solamente alle risorse elaborative locali ed alla rete internet.
- 7.20 La firma digitale viene di norma assegnata ai funzionari e loro sostituti, aventi potere di firma, specificando l'Ente di appartenenza (Comune di Cividale del Friuli); nel caso in cui l'assegnatario dello strumento di firma digitale cessi dal servizio presso il Comune di Cividale del Friuli, il titolare avrà cura di chiederne la cessazione, in pari data, al gestore del servizio; lo strumento di firma digitale, fisico, sarà restituito al Sistema Informativo Comunale, entro l'ultimo giorno di servizio, per la sua immediata distruzione fisica.
- 7.21 I sistemi anti-virus installati a protezione delle stazioni di lavoro assegnate, non possono essere disattivati se non a cura dell'Amministratore di Sistema per specifiche motivazioni.
- 7.22 L'archivio anagrafico è consultabile telematicamente da parte degli utenti autorizzati, in ossequio alla normativa vigente, mediante i sistemi tecnologici disponibili e con i profili di limitazione correlati alle esigenze del servizio.
- 7.23 Ogni postazione di lavoro è configurata in modo che:
- 7.23.1 alla richiesta dell'utente di accesso ad internet, il sistema si colleghi all'apposita pagina del portale web del Comune di Cividale del Friuli contenente il riepilogo dei sistemi gestionali in uso agli uffici/servizi del Comune di Cividale del Friuli.
  - 7.23.2 Nell'elenco dei "preferiti" dei browser di navigazione internet, siano presenti i collegamenti a tutti i sistemi gestionali in uso agli uffici/servizi del Comune di Cividale del Friuli.
- 7.24 gli utenti sono tenuti a memorizzare sui propri desktop i collegamenti a tutti i sistemi gestionali in uso al proprio ufficio/servizio, al fine di garantire una adeguata *business continuity* in caso di assenza di collegamento alla rete internet o al portale web del Comune di Cividale del Friuli.

I log relativi all'utilizzo di Strumenti, reperibili nella memoria degli Strumenti stessi ovvero sui Server o sui router dell'Ente, nonché i file con essi trattati sono registrati e possono essere oggetto di controllo da parte del Titolare del trattamento, attraverso l'Ufficio Sistema Informativo Comunale dell'Ente, per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio dell'Ente.

I controlli possono avvenire secondo le disposizioni previste al successivo punto 12 del presente Regolamento.

Le informazioni così raccolte sono altresì utilizzabili a tutti i fini connessi al rapporto di lavoro, compresa la verifica del rispetto del presente Regolamento, che costituisce adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli ai sensi del Regolamento Europeo 679/2016 "General Data Protection".

## 8 - Utilizzo di internet

Le regole di seguito specificate sono adottate anche ai sensi delle "Linee guida del Garante per posta elettronica e internet" pubblicate in Gazzetta Ufficiale n. 58 del 10 marzo 2007.

Ciascun dipendente /collaboratore si deve attenere alle seguenti regole di utilizzo della rete Internet e dei relativi servizi.

- 8.1 È ammessa solo la navigazione in siti considerati correlati con la prestazione lavorativa. L'accesso è consentito dal proxy dell'Ente con le sue policy di sicurezza debitamente implementate e aggiornate, ad esempio per i siti istituzionali, i siti degli Enti locali, di fornitori e partner dell'Ente. Il Comune di Cividale del Friuli si avvale di un sistema di *content filtering* fornito e gestito dalla Regione Autonoma Friuli Venezia Giulia.
- 8.2 È vietato compiere azioni che siano potenzialmente in grado di arrecare danno all'Ente, ad esempio, il download o l'upload di file audio e/o video, l'uso di servizi di rete con finalità ludiche o, comunque, estranee all'attività lavorativa.
- 8.3 È vietato a chiunque il download di qualunque tipo di software gratuito (freeware) o shareware prelevato da siti Internet, se non espressamente autorizzato dall'Amministratore di Sistema.
- 8.4 L'Ente si riserva la facoltà di bloccare l'accesso a siti "a rischio" anche di default, con l'uso del *content filtering*, attraverso l'utilizzo di blacklist pubbliche in continuo aggiornamento e di predisporre filtri, basati su sistemi euristici di valutazione del livello di sicurezza dei siti web remoti, tali da prevenire operazioni potenzialmente pericolose o comportamenti impropri.
- 8.5 Nel caso in cui, per ragioni di servizio, si necessiti di una navigazione libera dai filtri del suddetto proxy, è necessario richiedere lo sblocco all'Ufficio Sistema Informativo Comunale, nella quale siano indicati chiaramente: motivo della richiesta, utente e postazione da cui effettuare la navigazione libera, intervallo di tempo richiesto per completare l'attività. L'utente, nello svolgimento delle proprie attività, deve comunque tenere presente in modo particolare i punti 12 e 12.2 del presente regolamento. Al termine dell'attività gli incaricati dell'Ufficio Sistema Informativo Comunale ripristineranno i filtri nella situazione iniziale.
- 8.6 È vietata l'effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti on-line e simili, salvo i casi direttamente autorizzati dall'Ufficio Sistema Informativo Comunale, con il rispetto delle normali procedure di acquisto.

- 8.7 È vietato l'utilizzo di abbonamenti privati per effettuare la connessione a Internet tranne in casi del tutto eccezionali e previa autorizzazione dell'Amministratore di Sistema.
- 8.8 È vietata la partecipazione a Forum non professionali, ai Social Network, l'utilizzo di chat line (esclusi gli strumenti autorizzati), di bacheche elettroniche e le registrazioni in guest books anche utilizzando pseudonimi (o nicknames).
- 8.9 È consentito l'uso di strumenti di messaggistica istantanea, per permettere una efficace e comoda comunicazione tra i colleghi, mediante i soli strumenti autorizzati dall'Ufficio Sistema Informativo Comunale. Tali strumenti hanno lo scopo di migliorare la collaborazione tra utenti aggiungendo un ulteriore canale comunicativo rispetto agli spostamenti fisici, alle chiamate telefoniche ed e-mail. È consentito un utilizzo legato esclusivamente a scopi professionali. Anche su tali strumenti di messaggistica istantanea è attivo il monitoraggio e la registrazione dell'attività degli utenti, secondo le disposizioni dei punti 12 e 12.2 del presente regolamento.
- 8.10 Per motivi tecnici e di buon funzionamento del sistema informatico è buona norma, salvo comprovata necessità, non accedere a risorse web che impegnino in modo rilevante banda, come a titolo esemplificativo: filmati (tratti da youtube, siti di informazione, siti di streaming ecc) o web radio, in quanto possono limitare e/o compromettere l'uso della rete agli altri utenti.
- 8.11 E' autorizzata la gestione delle pagine, dei profili, dei blog e degli altri sistemi sui social networks, ufficialmente gestiti ed utilizzati dagli Uffici/Servizi Comunali, da parte degli operatori preposti. Tale autorizzazione deve intendersi estesa anche al personale formalmente iscritto al Gruppo Comunale Volontari di Protezione Civile, nonché agli Amministratori Comunali delegati al settore. In ogni caso trova applicazione il punto 14.6.
- 8.12 La creazione e registrazione di pagine, profili, blog ed altri sistemi sui social networks, quali strumenti di comunicazione ufficiale degli Uffici/Servizi Comunali, può avvenire esclusivamente utilizzando accounts istituzionali dell'Amministrazione Comunale.

Si informa che l'Ente, per il tramite dell'Ufficio Sistema Informativo Comunale, non effettua la memorizzazione sistematica delle pagine web visualizzate dal singolo Utente, né controlla con sistemi automatici i dati di navigazione dello stesso.

Si informa tuttavia che al fine di garantire il Servizio Internet e la sicurezza dei sistemi informativi, nonché per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio dell'Ente, l'Ente registra i dati di navigazione (file di log riferiti al traffico web) con modalità inizialmente volte a precludere l'immediata e diretta identificazione di Utenti, mediante opportune aggregazioni.

Solo in casi eccezionali e di comprovata urgenza rispetto alle finalità sopra descritte, l'Ente può trattare i dati di navigazione riferendoli specificatamente ad un singolo nome utente.

In tali casi i controlli avverranno nelle forme indicate al successivo punto 12 del presente Regolamento.

Le informazioni così raccolte sono altresì utilizzabili a tutti i fini connessi al rapporto di lavoro, compresa la verifica del rispetto del presente Regolamento, che costituisce adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli ai sensi del Regolamento Europeo 679/2016 "General Data Protection".

## 9 - Utilizzo della posta elettronica

Le regole di seguito specificate sono adottate anche ai sensi delle "Linee guida del Garante per posta elettronica e internet" pubblicate in Gazzetta Ufficiale n. 58 del 10 marzo 2007.

Ciascun dipendente/collaboratore si deve attenere alle seguenti regole di utilizzo dell'indirizzo di Posta elettronica.

- 9.1 Ad ogni utente viene fornito un account e-mail dell'Ente, nominativo, generalmente coerente con il modello nome.cognome@comune.cividale-del-friuli.ud.it ( alias pubblico nome.cognome@cividale.net ) l'utilizzo dell'e-mail deve essere limitato esclusivamente a scopi e finalità dell'Ente, ed è assolutamente vietato ogni utilizzo privato. L'utente a cui è assegnata una casella di posta elettronica è responsabile del corretto utilizzo della stessa.
- 9.2 L'Ente fornisce, altresì, delle caselle di posta elettronica associate a ciascuna unità organizzativa, ufficio o gruppo di lavoro (coerenti con il modello ufficio@comune.cividale-del-friuli.ud.it , alias pubblico ufficio@cividale.net ) il cui utilizzo è da preferire rispetto alle e-mail nominative qualora le comunicazioni siano di interesse collettivo: questo per evitare che degli utenti singoli mantengano l'esclusività su dati dell'Ente. Il Responsabile dell'Unità Operativa di riferimento individua più operatori, per ciascuna di tali caselle, da abilitare alla loro gestione; operatori che saranno abilitati dall'Ufficio del Sistema Informativo Comunale ad accedere a tale casella, con le proprie medesime credenziali di accesso alla rete comunale.
- 9.3 Ciascuna casella di posta elettronica deve essere configurata in modo che, in calce ad ogni messaggio, siano sempre riportate le generalità del mittente, il ruolo, il servizio/ufficio e l'Amministrazione di appartenenza, i recapiti telefonici fissi e cellulari (di servizio), fax ed e-mail (dell'ufficio di appartenenza) e la seguente nota di riservatezza:  
"AVVERTENZA: INFORMATIVA SUL TRATTAMENTO DEI DATI  
Questo messaggio, comprensivo di eventuali allegati, è ad uso esclusivo del destinatario e potrebbe contenere informazioni riservate. Qualora venisse ricevuto per errore, si prega di provvedere alla sua distruzione e di darne notizia al mittente. Si informa che un eventuale trattamento di dati personali contenuti nella presente comunicazione, in assenza dei presupposti di liceità previsti dall'art 6 Reg. 679/16 (GDPR), è punito secondo la normativa vigente in materia."  
Si informa che la casella di posta elettronica è di titolarità del Comune di Cividale del Friuli ed è concessa ai propri dipendenti e collaboratori esclusivamente per rendere la prestazione lavorativa."
- 9.4 La casella di Posta Elettronica Certificata istituzionale dell'Ente (pubblicata sul portale internet dell'Amministrazione Comunale) è integrata nel Protocollo Informatico del Comune di Cividale del Friuli.
- 9.5 L'iscrizione a mailing-list o newsletter esterne con il proprio indirizzo dell'Ente personale è concessa esclusivamente per motivi professionali. Prima di iscriversi occorre verificare anticipatamente l'affidabilità del sito che offre il servizio.
- 9.6 Allo scopo di garantire sicurezza alla rete dell'Ente, evitare di aprire messaggi di posta in arrivo da mittenti di cui non si conosce l'identità o con contenuto sospetto o insolito, oppure che contengano allegati di tipo \*.exe, \*.com, \*.vbs, \*.htm, \*.scr, \*.bat, \*.js e \*.pif. È necessario porre molta attenzione, inoltre, alla credibilità del messaggio e del mittente per evitare casi di phishing o frodi informatiche. In qualunque situazione di incertezza contattare l'Amministratore di Sistema per una valutazione dei singoli casi.

- 9.7 Non é consentito diffondere messaggi del tipo "catena di S. Antonio" o di tipologia simile anche se il contenuto sembra meritevole di attenzione; in particolare gli appelli di solidarietà e i messaggi che informano dell'esistenza di nuovi virus. In generale è vietato l'invio di messaggi pubblicitari di prodotti di qualsiasi tipo.
- 9.8 Nel caso fosse necessario inviare allegati "pesanti" è opportuno ricorrere prima alla compressione dei file originali in un archivio di formato .zip o equivalenti. Nel caso di allegati ancora più voluminosi è necessario utilizzare lo specifico strumento di trasmissione reso disponibile dall'Ufficio Sistema Informativo Comunale.
- 9.9 Nel caso in cui fosse necessario inviare a destinatari esterni messaggi contenenti dati personali relativi allo stato di salute, in particolare se l'invio non è occasionale, è raccomandato che questi dati vengano preventivamente resi inintelligibili attraverso criptazione con apposito software (archiviazione e compressione con password). La password di crittazione deve essere comunicata al destinatario attraverso un canale diverso dalla mail (ad esempio per lettera o per telefono) e mai assieme ai dati criptati. Tutte le informazioni dell'Ente, i dati personali e/o sensibili di competenza dell'Ente possono essere inviati soltanto a destinatari - persone o Enti – qualificati, competenti ed autorizzati a tale trattamento.
- 9.10 Non è consentito l'invio automatico di e-mail, dalla casella istituzionale all'indirizzo e-mail privato (attivando per esempio un "inoltrato" automatico delle e-mail entranti), anche durante i periodi di assenza (es. ferie, malattia, infortunio ecc.). In questa ultima ipotesi, sull'account e-mail dell'Ente nominativo, dovrà essere inserito un messaggio di cortesia "Out of Office", facendo menzione di chi o quale struttura, all'interno dell'Ente, assumerà le mansioni durante l'assenza ed indicando almeno un indirizzo e-mail alternativo di tipo collettivo, tipo [ufficio@cividale.net](mailto:ufficio@cividale.net) . L'invio automatico di e-mail, dalla casella istituzionale all'indirizzo e-mail privato (attivando per esempio un "inoltrato" automatico delle e-mail entranti), è consentito esclusivamente sulle caselle e-mail fornite agli Amministratori dell'Ente (Assessori e Consiglieri Comunali), con attivazione da richiedere all'Ufficio Sistema Informativo Comunale, da aggiornare ad ogni mutazione degli Amministratori dell'Ente.
- 9.11 In caso di assenza improvvisa o prolungata e per improrogabili necessità legate all'attività lavorativa, qualora non fosse possibile attivare la funzione auto-reply o l'inoltrato automatico su altre caselle dell'Ente e si debba conoscere il contenuto dei messaggi di posta elettronica, il titolare della casella di posta ha la facoltà di delegare un altro dipendente (fiduciario) per verificare il contenuto di messaggi e per inoltrare al titolare del trattamento quelli ritenuti rilevanti per lo svolgimento dell'attività lavorativa. Sarà compito del Responsabile dell'Unità Operativa di assegnazione assicurarsi che sia redatto un verbale attestante quanto avvenuto e che sia informato il lavoratore interessato alla prima occasione utile;
- 9.12 La diffusione massiva di messaggi di posta elettronica deve essere effettuata esclusivamente per motivi inerenti il servizio, su autorizzazione del Responsabile della Unità Operativa competente. Per evitare che le eventuali risposte siano inoltrate a tutti, generando traffico eccessivo ed indesiderato, i destinatari dovranno essere messi in copia nascosta (Bcc o Ccn), se la tipologia del messaggio lo consente.
- 9.13 È vietato inviare posta elettronica in nome e per conto di un altro utente;
- 9.14 Ogni casella di posta elettronica – trattandosi di mero sistema di veicolazione delle informazioni - deve essere mantenuta in ordine, cancellando messaggi e documenti la cui conservazione non è più necessaria. La conservazione di messaggi con allegati è sempre da evitare, provvedendo al tempestivo salvataggio dell'allegato sulle condivisioni dell'Ente.

- 9.15 Tutta la corrispondenza istituzionale sarà inviata direttamente, dagli utenti che intendano avvalersi dei servizi dell'Ente, all'indirizzo di posta elettronica certificata (PEC) del Comune di Cividale del Friuli.
- 9.16 I messaggi in entrata vengono sistematicamente analizzati alla ricerca di virus e malware e per l'eliminazione dello spam. I messaggi che dovessero contenere virus vengono eliminati dal sistema e il mittente/destinatario viene avvisato mediante messaggio specifico. Tali adempimenti sono svolti, in forma centralizzata, dal sistema convenzionato con la Regione Autonoma Friuli Venezia Giulia.
- 9.17 Qualora per intrattenere rapporti con l'utenza sia utilizzata in fase interlocutoria la propria e-mail personale istituzionale, dovrà essere specificato che l'invio della corrispondenza ufficiale indirizzata al Comune ed oggetto di protocollazione dovrà avvenire esclusivamente tramite la casella di Posta Elettronica Certificata (PEC), senza doppi passaggi.

Si informa che le comunicazioni anche elettroniche ed i documenti elettronici allegati possono avere rilevanza procedimentale e pertanto devono essere conservate per la durata prevista dalla normativa vigente.

Si informa altresì che l'Ente, per il tramite dell'Ufficio Sistema Informativo Comunale, non controlla sistematicamente il flusso di comunicazioni mail né è dotato di sistemi per la lettura o analisi sistematica dei messaggi di posta elettronica ovvero dei relativi dati esteriori, al di là di quanto tecnicamente necessario per svolgere il servizio e-mail.

Tuttavia, in caso di assenza improvvisa o prolungata del dipendente ovvero per imprescindibili esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio dell'Ente ovvero per motivi di sicurezza del sistema informatico, l'Ente per il tramite dell'Ufficio Sistema Informativo Comunale può, secondo le procedure indicate successivo punto 12 del presente Regolamento, accedere all'account di posta elettronica dell'Ente, prendendo visione dei messaggi, salvando o cancellando file.

Si informa che, in caso di cessazione del rapporto lavorativo, la mail dell'Ente affidata all'incaricato verrà sospesa per un periodo di **6 mesi** e successivamente disattivata. Nel periodo di sospensione l'account rimarrà attivo e visibile ad un soggetto incaricato dall'Ente solo in ricezione, che tratterà i dati e le informazioni pervenute per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio dell'Ente, trasmettendone il contenuto ad altri dipendenti (se il messaggio ha contenuto lavorativo) ovvero cancellandolo (se il messaggio non ha contenuto lavorativo). Il sistema in ogni caso genererà una risposta automatica al mittente, invitandolo a reinviare il messaggio ad altro indirizzo mail dell'Ente.

Le informazioni eventualmente raccolte sono altresì utilizzabili a tutti i fini connessi al rapporto di lavoro, compresa la verifica del rispetto del presente Regolamento, che costituisce adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli ai sensi del Regolamento Europeo 679/2016 "General Data Protection".

## **10 - Utilizzo dei telefoni, fax, fotocopiatrici, scanner e stampanti**

Il dipendente è consapevole che gli Strumenti di stampa, così come anche il telefono dell'Ente, sono di proprietà del Comune di Cividale del Friuli e sono resi disponibili all'utente per rendere la prestazione lavorativa. Pertanto ne viene concesso l'uso esclusivamente per tale fine.

- 10.1 Il telefono dell'Ente affidato all'utente è uno strumento di lavoro. Ne viene concesso l'uso esclusivamente per lo svolgimento dell'attività lavorativa e non sono quindi consentite comunicazioni a carattere personale e/o non strettamente inerenti l'attività lavorativa stessa. La ricezione o l'effettuazione di comunicazioni a carattere personale è consentita solo nel caso di comprovata necessità ed urgenza, per il limitato tempo strettamente necessario alla comunicazione stringata, specifica ed essenziale, limitazioni in essere anche per l'utilizzo di apparati cellulari/smartphone privati, in orario di servizio.
- 10.2 Al fine di garantire un corretto utilizzo dei servizi di telefonia (VoIP, mobile, ecc.) l'Ente predispone, ove tecnicamente possibile, adeguate configurazioni dei sistemi che consentano l'effettuazione o meno delle diverse tipologie di chiamata (es. chiamate su telefonini, internazionali etc.).
- 10.3 Accesso ai dati trattati dall'utente: per motivi di sicurezza del sistema telefonico, per motivi tecnici e/o manutentivi e programmazione dei costi, comunque estranei a qualsiasi finalità di controllo dell'attività lavorativa, è facoltà dell'Ufficio Patrimonio, tramite l'Amministratore di Sistema, accedere direttamente, nel rispetto della normativa sulla protezione dei dati, a tutti gli strumenti di telecomunicazione aziendali.
- 10.4 La Regione Autonoma Friuli Venezia Giulia garantisce, per le finalità di accertamento e repressione dei reati, la conservazione dei dati di traffico telefonico entro il limite di 72 (settantadue) mesi, ai sensi dell'articolo 24, Comma 1, della Legge 167/2017.
- 10.5 Il sistema telefonico VoIP in uso, è reso disponibile dalla Regione Autonoma Friuli Venezia Giulia; le misure di sicurezza e protezione informatica, anche al data-base con i dati trattati, sono a carico di tale gestore ed erogatore di servizio.
- 10.6 Gli utenti del sistema telefonico devono intendersi adeguatamente informati in forza delle indicazioni riportate nel presente Regolamento.
- 10.7 Nei periodi di assenza programmata ogni operatore, sulla scorta delle indicazioni fornite dal Responsabile della Unità Operativa, avrà cura di deviare la propria linea telefonica fissa su altra terminazione, ove regolarmente presidiata, dell'Ufficio/servizio di appartenenza.
- 10.8 Nei casi di assegnazione di un cellulare dell'Ente all'utente, quest'ultimo sarà responsabile del suo utilizzo e della sua custodia. Ai cellulari e smartphone dell'Ente si applicano le medesime regole sopra previste per gli altri dispositivi informatici (cfr. 7 "Utilizzo di personal computer"), per quanto riguarda il mantenimento di un adeguato livello di sicurezza informatica. In particolare si raccomanda il rispetto delle regole per una corretta navigazione in Internet (cfr. 8), se consentita.
- 10.9 Per gli smartphone dell'Ente è vietata l'installazione e l'utilizzo di applicazioni (o altresì denominate "app" nel contesto degli smartphone) diverse da quelle autorizzate dal Sistema Informativo Comunale.
- 10.10 La creazione di gruppi condivisi (anche su WhatsApp o servizi simili) per lo svolgimento di attività istituzionali, potrà avvenire solamente includendovi dispositivi di servizio, non potendo essere inclusi apparati privati. In ogni caso i messaggi trasmessi devono risultare inerenti l'attività lavorativa.
- 10.11 È vietato l'utilizzo delle fotocopiatrici per finalità non istituzionali dell'Ente.
- 10.12 Per quanto concerne l'uso delle stampanti gli utenti sono tenuti a:
  - 10.12.1 Stampare documenti solo se strettamente necessari per lo svolgimento delle proprie funzioni operative.
  - 10.12.2 Prediligere le stampanti di rete condivise, rispetto a quelle locali/personali, per ridurre l'utilizzo di materiali di consumo (toner ed altri consumabili).



- 10.12.3 Prediligere la stampa in bianco/nero e fronte/retro al fine di ridurre i costi.
- 10.12.4 Evitare di stampare la corrispondenza digitale già registrata nel Protocollo Informatico, strumento conforme alle regole del CAD (Codice Amministrazione Digitale) anche per quanto inerente la conservazione sostitutiva.
- 10.12.5 Evitare di archiviare copie digitali della corrispondenza già registrata nel Protocollo Informatico, strumento conforme alle regole del CAD (Codice Amministrazione Digitale) anche per quanto inerente la conservazione sostitutiva.
- 10.13 Le stampanti e le fotocopiatrici dell'Ente devono essere spente ogni sera prima di lasciare gli uffici o in caso di inutilizzo prolungato.
- 10.14 Al fine di evitare la divulgazione di informazioni a persone terze non autorizzate, il rilascio delle stampe inviate sulle stampanti di gruppo avverrà solo previo digitazione di apposita password personale e segreta attribuita ad ogni utente.
- 10.15 L'utilizzo del fax deve intendersi come sistema di comunicazione residuale, limitatamente nei confronti di entità privatistiche, essendo obbligatorio l'utilizzo della comunicazione digitale (posta elettronica o connessioni telematiche dirette) nei rapporti tra Pubbliche Amministrazioni. I fax in arrivo al numero principale del Comune di Cividale del Friuli, sono automaticamente digitalizzati ed inoltrati alla casella di Posta Elettronica Certificata del Comune di Cividale del Friuli, integrata nel Protocollo.
- 10.16 Tutti i documenti acquisiti tramite sistemi scanner/multifunzione, dovranno essere tempestivamente rimossi, o cancellati, dagli archivi locali, nello stretto tempo necessario al loro trasferimento nelle cartelle di rete del Sistema Informativo Comunale.

## **11 - Assistenza agli utenti e manutenzioni**

- 11.1 L'Ufficio del Sistema informativo Comunale, per il tramite dell'Amministratore di Sistema, può accedere ai dispositivi informatici dell'Ente sia direttamente, sia mediante software di accesso remoto, per i seguenti scopi:
  - 11.1.1 – verifica e risoluzione di problemi sistemistici ed applicativi, su segnalazione dell'utente finale.
  - 11.1.2 – verifica del corretto funzionamento dei singoli dispositivi in caso di problemi rilevati nella rete.
  - 11.1.3 – richieste di aggiornamento software e manutenzione preventiva hardware e software.
- 11.2 Gli interventi tecnici possono avvenire previo consenso dell'utente, quando l'intervento stesso richiede l'accesso ad aree personali dell'utente stesso. Qualora l'intervento tecnico in loco o in remoto non necessiti di accedere mediante credenziali utente, gli Amministratori di sistema sono autorizzati ad effettuare gli interventi senza il consenso dell'utente cui la risorsa è assegnata.
- 11.3 L'accesso in teleassistenza sui PC della rete dell'Ente richiesto da terzi (fornitori e/o altri) deve essere autorizzato dall'Amministratore di Sistema, per le verifiche delle modalità di intervento per il primo accesso. Le richieste successive, se effettuate con la medesima modalità, possono essere gestite autonomamente dall'utente finale.
- 11.4 Durante gli interventi in teleassistenza da parte di operatori terzi, l'utente richiedente o l'Amministratore di Sistema devono presenziare la sessione remota, in modo tale da verificare ed impedire eventuali comportamenti non conformi al presente regolamento.

## 12 - Verifiche sugli Strumenti (art. 6.1 Provv. Garante, ad integrazione dell'Informativa ex art. 13 Reg. 679/16)

12.1 Poiché in caso di violazioni contrattuali e giuridiche, sia l'Ente, sia il singolo lavoratore sono potenzialmente perseguibili con sanzioni, anche di natura penale, l'Ente verificherà, nei limiti consentiti dalle norme legali e contrattuali, il rispetto delle regole e l'integrità del proprio sistema informatico. L'Amministratore di Sistema provvederà quindi alla verifica delle eventuali anomalie riscontrate sul Sistema Informativo Comunale provvedendo in merito, nei limiti consentiti dalle norme legali e contrattuali. Resta ferma la necessità di rispettare le procedure di informazione e di consultazione di lavoratori e sindacati in relazione all'introduzione o alla modifica di sistemi automatizzati per la raccolta e l'utilizzazione dei dati, nonché in caso di introduzione o di modificazione di procedimenti tecnici destinati a controllare i movimenti o la produttività dei lavoratori. Le verifiche devono essere effettuate nel rispetto del Regolamento UE 2016/679, del presente Regolamento e dei seguenti principi:

- **Proporzionalità:** il controllo e l'estensione dello stesso dovrà rivestire, in ogni caso, un carattere adeguato, pertinente e non eccessivo rispetto alla/alle finalità perseguite, ma resterà sempre entro i limiti minimi.
- **Trasparenza:** l'adozione del presente Regolamento ha l'obiettivo di informare gli utenti sui diritti ed i doveri di entrambe le parti.
- **Pertinenza e non eccedenza:** ovvero evitando un'interferenza ingiustificata sui diritti e sulle libertà fondamentali dei lavoratori, così come la possibilità di controlli prolungati, costanti o indiscriminati.

12.2 Si evidenzia che l'uso degli Strumenti Informatici dell'Ente può lasciare traccia delle informazioni sul relativo uso, come analiticamente spiegato nei riquadri di cui ai punti 6 – 7 – 8 – 9 del presente Regolamento. Tali informazioni, che possono contenere dati personali eventualmente anche sensibili dell'Utente, possono essere oggetto di controlli da parte dell'Ente, per il tramite dell'Amministratore di Sistema, volti a garantire esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio dell'Ente, nonché per la sicurezza e la salvaguardia del sistema informatico, per ulteriori motivi tecnici e/o manutentivi (ad es. aggiornamento / sostituzione / implementazione di programmi, manutenzione hardware, etc.). Gli interventi di controllo sono di due tipi (di seguito descritti al punto 12.3 e 12.4) e possono permettere all'Ente di prendere indirettamente cognizione dell'attività svolta con gli strumenti.

12.3 **Controlli per la tutela del patrimonio dell'Ente, nonché per la sicurezza e la salvaguardia del sistema informatico. Controlli per ulteriori motivi tecnici e/o manutentivi (ad es. aggiornamento/sostituzione/implementazione di programmi, manutenzione hardware, ecc.).**

Qualora per le finalità qui sopra descritte risulti necessario l'accesso agli Strumenti e alle risorse informatiche e relative informazioni descritte ai punti 6 – 7 – 8 – 9 il Responsabile del trattamento dei dati personali per il tramite dell'Ufficio Sistema Informativo Comunale, si atterrà al processo descritto qui di seguito (se e in quanto compatibile con lo Strumento oggetto di controllo).

- i. Avviso generico a tutti i dipendenti della presenza di comportamenti anomali che possono mettere a rischio la sicurezza del sistema informativo e richiamo all'esigenza di attenersi al rispetto del presente Regolamento.
- ii. Successivamente, dopo almeno 7 giorni, se il comportamento anomalo persiste, l'Ente potrà autorizzare il personale addetto al controllo, potendo così accedere alle informazioni descritte ai punti 6 – 7 – 8 – 9 con possibilità di rilevare files trattati, siti web visitati, software installati, documenti scaricati, statistiche sull'uso di risorse

ecc. nel corso dell'attività lavorativa. Tale attività potrà essere effettuata in forma anonima ovvero tramite controllo del numero IP, dell'Utente e con l'identificazione del soggetto che non si attiene alle istruzioni impartite.

- iii. Qualora il rischio di compromissione del sistema informativo dell'Ente sia imminente e grave a tal punto da non permettere l'attesa dei tempi necessari per i passaggi procedurali descritti ai punti 1 e 2, il Responsabile del Trattamento, unitamente all'amministratore di sistema, può intervenire senza indugio sullo strumento da cui proviene la potenziale minaccia.

#### **12.4 Controlli per esigenze produttive e di organizzazione**

Per esigenze produttive e di organizzazione si intendono – fra le altre – l'urgente ed improrogabile necessità di accedere a files o informazioni lavorative di cui si è ragionevolmente certi che siano disponibili su risorse informatiche di un Utente (quali file salvati, posta elettronica, chat, SMS, ecc) che non sia reperibile, in quanto ad esempio assente, temporaneamente irreperibile ovvero cessato.

Qualora risulti necessario l'accesso alle risorse informatiche e relative informazioni descritte ai punti 6 – 7 – 8 – 9 il Responsabile del trattamento dei dati personali, per il tramite dell'Ufficio Sistema informativo Comunale, si atterrà alla procedura descritta qui di seguito (se e in quanto compatibile con lo Strumento oggetto di controllo).

- i. Redazione di un atto da parte del Responsabile dell'Unità Operativa che comprovi le necessità produttive e di organizzazione che richiedano l'accesso allo Strumento.
- ii. Incarico all'Amministratore di sistema di accedere alla risorsa con credenziali di Amministratore ovvero tramite l'azzeramento e la contestuale creazione di nuove credenziali di autenticazione dell'Utente interessato, con avviso che al primo accesso alla risorsa, lo stesso dovrà inserire nuove credenziali.
- iii. Redazione di un verbale che riassume i passaggi precedenti.
- iv. In ogni caso l'accesso ai documenti presenti nella risorsa è limitato a quanto strettamente indispensabile alle finalità produttive e di organizzazione del lavoro.
- v. Qualora indirettamente si riscontrino file o informazioni anche personali, esse potranno essere altresì utilizzabili a tutti i fini connessi al rapporto di lavoro, considerato che il presente Regolamento costituisce adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli, sempre nel rispetto di quanto disposto dal Regolamento Europeo 679/2016 "General Data Protection".

Tutti i controlli sopra descritti avvengono nel rispetto del principio di necessità e non eccedenza rispetto alle finalità descritte nel presente Regolamento. Dell'attività sopra descritta viene redatto verbale, sottoscritto dal Responsabile del Trattamento e dall'Amministratore di Sistema che ha svolto l'attività.

In caso di nuovo accesso da parte dell'utente allo Strumento informatico oggetto di controllo, lo stesso dovrà avvenire previo rilascio di nuove credenziali (salvo diverse esigenze tecniche).

Qualora indirettamente si riscontrino file o informazioni anche personali, esse potranno essere altresì utilizzabili a tutti i fini connessi al rapporto di lavoro, considerato che il presente Regolamento costituisce adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli, sempre nel rispetto di quanto disposto dal Regolamento Europeo 679/2016 "General Data Protection".

### **13- Conservazione dei dati**

- 13.1 In riferimento agli articoli 5 e 6 del Reg. 679/2016 e in applicazione ai principi di diritto di accesso, legittimità, proporzionalità, sicurezza ed accuratezza e conservazione dei dati, le informazioni relative all'accesso ad Internet e dal traffico telematico (log di sistema e del server proxy), la cui conservazione non sia necessaria, saranno cancellati entro 6 (sei) mesi al massimo, salvo esigenze tecniche o di sicurezza; o per l'indispensabilità dei dati rispetto all'esercizio o alla difesa di un diritto in sede giudiziaria o, infine, all'obbligo di custodire o consegnare i dati per ottemperare ad una specifica richiesta dell'autorità giudiziaria o della polizia giudiziaria.
- 13.2 L'Ente si impegna ad assumere le misure di sicurezza nel trattamento e nella conservazione di tale tipologia di dati alla luce di quanto stabilito dal Legislatore. Obblighi in capo alla Regione Autonoma Friuli Venezia Giulia, nel contesto del Protocollo d'intesa in essere in materia informatica.

### **14 - Partecipazione ai Social Media**

- 14.1 L'utilizzo a fini istituzionali dei social media (Facebook, Instagram, LinkedIn, Twitter, Youtube, ecc., dei blog e dei forum, anche professionali ed altri siti) è gestito ed organizzato esclusivamente dall'Ente attraverso specifiche direttive ed istruzioni operative al personale a ciò espressamente addetto, rimanendo escluse iniziative individuali da parte dei singoli utenti, collaboratori o Uffici.
- 14.2 Fermo restando il diritto della persona alla libertà di espressione, l'Ente ritiene comunque opportuno indicare agli utenti alcune regole comportamentali, al fine di tutelare tanto la propria immagine ed il patrimonio dell'Ente, anche immateriale, quanto i propri collaboratori, i propri utenti e fornitori, oltre che gli stessi utenti utilizzatori dei social media.
- 14.3 Il presente articolo deve essere osservato dall'Utente sia che utilizzi dispositivi messi a disposizione dall'Ente, sia che utilizzi propri dispositivi, sia che partecipi ai social media a titolo personale, sia che lo faccia per finalità professionali come dipendente del Comune di Cividale del Friuli.
- 14.4 E' vietata la partecipazione ai social media durante l'orario di servizio, per finalità personali.
- 14.5 La condivisione dei contenuti nei social media deve sempre rispettare e garantire la segretezza sulle informazioni dell'Ente, nel rispetto del segreto d'ufficio, segreto professionale e privacy.
- 14.6 L'utilizzo dei social media è interdetto agli utenti/collaboratori sulla rete informatica del Comune di Cividale del Friuli; deroghe potranno essere concesse a singoli utenti, previo motivata richiesta del Responsabile dell'Unità Operativa all'Ufficio Sistema Informativo Comunale, addetti alla gestione delle pagine, dei profili, dei blogs o altri contenuti presenti sui social networks, registrati quali strumenti ufficiali di comunicazione degli Uffici/Servizi dell'Amministrazione Comunale.

### **15 – Attività Sindacali e R.S.U.**

- 15.1 Nell'ambito dell'agibilità sindacale prevista dal CCRL vigente è consentito l'uso di tutte le apparecchiature a disposizione dell'Ente (Personal Computers, stampanti, fotocopiatrici, scanner, caselle di posta elettronica, accesso internet, ecc.), senza limitazioni od oneri a carico, per l'espletamento dell'attività sindacale da parte delle RSU elette, Dirigenti sindacali o personale dipendente individuato

dalle organizzazioni sindacali territoriali che operano nell'ambito dell'Amministrazione Comunale di Cividale del Friuli, per fini sindacali.

## **16 - Sanzioni disciplinari**

16.1 È fatto obbligo a tutti i dipendenti/collaboratori/utenti di osservare le disposizioni portate a conoscenza con il presente Regolamento.

## **17 - Entrata in vigore**

17.1 Il presente regolamento sarà operativo ed efficace per tutti i destinatari a partire dall'avvenuta pubblicazione all'Albo Pretorio della Delibera di adozione.

## **18 – Divulgazione**

18.1 Copia del presente documento sarà inoltrato alla casella e-mail istituzionale di ciascun operatore del Comune di Cividale del Friuli, agli Amministratori Comunali aventi accesso al sistema informatico, alle ditte incaricate dell'assistenza informatica e pubblicato sul sito internet istituzionale del Comune.