COMUNE DI CITTADELLA

Cittadella Città d'Arte

PROVINCIA DI PADOVA

VERBALE DI DELIBERAZIONE DELLA GIUNTA COMUNALE

Deliberazione n. 187 del 12/07/2019

OGGETTO: APPROVAZIONE DISCIPLINARE PER L'UTILIZZO DELLE RISORSE INFORMATICHE E TELEFONICHE DEL COMUNE DI CITTADELLA.

L'anno **duemiladiciannove** il giorno **dodici** del mese di **luglio** alle ore **11:00** in Cittadella, nella sala delle adunanze la Giunta Comunale si è riunita con la presenza dei Signori:

PIEROBON LUCA	SINDACO	Presente
SIMIONI MARCO	ASSESSORE	Presente
BELTRAME MARINA	ASSESSORE	Presente
GALLI DIEGO	ASSESSORE	Presente
PAVAN FRANCESCA	ASSESSORE	Presente
DE ROSSI FILIPPO	ASSESSORE	Assente

Presenti n. 5 **Assenti n. 1**

Partecipa alla seduta il VICE SEGRETARIO SARTORE CARLO che provvede alla redazione del presente verbale.

Assume la presidenza il Sig. PIEROBON LUCA, nella sua qualità di SINDACO, il quale riconosciuta legale l'adunanza, dichiara aperta la seduta ed invita i presenti a deliberare sull'oggetto sopra indicato.

Deliberazione n. 187 del 12/07/2019

Viene esaminata la seguente proposta di delibera redatta dal Responsabile del Servizio, sulla quale sono stati espressi i pareri ai sensi dell'art. 49, comma 1 del D. Lgs. 267/2000.

OGGETTO: APPROVAZIONE DISCIPLINARE PER L'UTILIZZO DELLE RISORSE INFORMATICHE E TELEFONICHE DEL COMUNE DI CITTADELLA.

LA GIUNTA COMUNALE

CONSIDERATO che:

- la diffusione delle tecnologie informatiche e telematiche ed il progressivo passaggio della società verso modelli di comunicazione sempre più integrati ed interconnessi, rende fondamentale per ogni realtà organizzativa e lavorativa, lo sviluppo di una cultura della sicurezza del proprio patrimonio informativo e della tutela dei diritti degli interessati;
- è dovere dell'Ente individuare il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza che configurano il livello minimo di protezione per il trattamento dei dati personali, nonché adottare idonee misure di sicurezza per assicurare la disponibilità e l'integrità di sistemi informativi, anche per prevenire utilizzi indebiti che possono essere fonte di responsabilità;
- la normativa vigente in materia di Privacy e sicurezza Regolamento Europeo 2016/679 (artt. 24 e 32) e successivo D.Lgs. 101/2018 adottato a modifica del D.Lgs. 196/2003 e la circolare AGID 2/2017, forniscono indicazioni operative per l'adozione e la verifica di misure di sicurezza tecniche ed organizzative per la tutela del dato personale e delle condizioni minime di sicurezza ICT relativamente al trattamento dei dati;

RITENUTO che l'elevato uso della tecnologia informatica (e in particolare l'accesso alla rete informatica e telematica, Internet e posta elettronica) come strumento di lavoro in questo Comune, impone la necessità di regolamentarne l'utilizzo, allo scopo di fornire agli utenti, (dipendenti, amministratori e collaboratori) adeguata informazione circa le modalità da seguire per un corretto utilizzo degli strumenti e delle risorse informatiche e telematiche messe loro a disposizione per lo svolgimento delle proprie mansioni istituzionali, in modo che possano collaborare alle politiche di sicurezza messe in atto;

RITENUTO inoltre di porre in essere adeguati e commisurati sistemi di controllo sul corretto utilizzo degli strumenti e delle risorse informatiche e telematiche, senza che ciò possa in alcun modo invadere e violare la sfera personale del lavoratore e quindi il suo diritto alla riservatezza ed alla dignità come sancito dallo Statuto dei Lavoratori e dal D.Lgs. 196/03;

VISTO il "Disciplinare per l'utilizzo delle risorse informatiche e telefoniche del Comune di Cittadella", che si allega alla presente deliberazione per farne parte integrante e sostanziale;

PRECISATO che tale disciplinare:

- si conforma alle indicazioni fornite dal Garante per la Protezione dei dati personali che con deliberazione n. 13 del 1 marzo 2007, ha emanato le linee guida in materia di utilizzo di strumenti informatici e telematici, nonché della posta elettronica e della rete Internet, nel rapporto di lavoro, oltre alla normativa in vigore;
- si configura come strumento a tutela dei diritti patrimoniali dell'Ente ed a garanzia della sicurezza ed integrità del proprio patrimonio informativo;
- si caratterizza come strumento di garanzia a favore di tutti coloro che svolgono un rapporto di lavoro o di servizio a beneficio dell'Ente, nella misura in cui costituisce una informativa preventiva, fornita a tutti questi soggetti, circa termini, casi e modalità di verifica del corretto utilizzo degli strumenti informatici e telematici messi a loro disposizione per le attività di lavoro o di servizio;

RITENUTO di adottare l'allegato "Disciplinare per l'utilizzo delle risorse informatiche e telefoniche del Comune di Cittadella", dando atto che lo stesso dovrà essere reso noto a tutti i dipendenti con le forme più efficaci ed immediate;

VISTO il D. Lgs. 267/2000 recante il Testo Unico sull'Ordinamento degli Enti Locali";

DELIBERA

1. di adottare, per tutto quanto in premessa indicato e qui inteso come integralmente riportato, l'allegato "Disciplinare per l'utilizzo delle risorse informatiche e telefoniche del Comune di Cittadella", parte integrante e sostanziale del presente atto
2. di attestare la pubblicazione di cui all'art. 23 del D.Lgs. 33/2013;
3. di dare atto dell'avvenuto assolvimento degli obblighi di astensione di cui agli artt. 5 e 6 del codice di comportamento approvato con deliberazione di Giunta Comunale n. 12/2014 e dell'art. 6-bis della L. 241/90 e, pertanto, in ordine al presente provvedimento non sussiste situazione di conflitto di interessi né in capo al responsabile del procedimento, né in capo ai soggetti che sottoscrivono a vario titolo il presente atto, né in capo a chi partecipa, a qualsiasi titolo a detto procedimento;
4. di dichiarare con votazione autonoma e separata la presente deliberazione immediatamente eseguibile ai sensi e per gli effetti dell'art. 134 del Decreto Legislativo n. 267/2000.

LA GIUNTA COMUNALE

Vista la su estesa proposta di delibera;

Avuti i prescritti pareri favorevoli a termini ai sensi dell'art. 49, 1° comma del decreto legislativo 18.08.2000 n. 267, “Testo Unico delle leggi sull'ordinamento degli Enti Locali” espressi sulla proposta di delibera e riportati a conferma in calce alla presente;

Con voti unanimi e favorevoli, palesemente espressi

DELIBERA

1 di approvare e far propria la proposta di delibera sopra riportata nella sua formulazione integrale, ovvero senza alcuna modificazione o integrazione;

2 di comunicare la presente delibera ai capigruppo consiliari ai sensi dell'art. 125 del D. Lgs. 267/2000.

*****

Con apposita votazione, favorevole ed unanime, il presente atto è dichiarato immediatamente eseguibile ai sensi dell'art. 134 comma 4 del D.Lgs 267/2000.

COMUNE DI CITTADELLA

Cittadella Città d'Arte

PROVINCIA DI PADOVA

Letto, approvato e sottoscritto digitalmente ai sensi dell'art. 21 D.L.gs n 82/2005 e s.m.i.

Verbale n. **32** del **12**.**07**.**2019**

IL SINDACO
PIEROBON LUCA

IL VICE SEGRETARIO
SARTORE CARLO

COMUNE DI CITTADELLA

Cittadella Città d'Arte

PROVINCIA DI PADOVA

DISCIPLINARE PER

L'UTILIZZO DELLE

RISORSE INFORMATICHE

E TELEFONICHE DEL COMUNE DI CITTADELLA

Approvato con Delibera di Giunta

n. _____ del _____

Palazzo Mantegna – Via Indipendenza, 41 – 35013 Cittadella (PD)
P.I 00731540282 – C.F. 81000370288 – Tel. 049-9413411 – www.comune cittadella.pd.it

INDICE

Changelog

Versione	Data	Cambiamenti effettuati dall'ultima versione
1.0	01/07/2019	Stesura iniziale

Premessa

Il presente disciplinare intende fornire ai dipendenti, amministratori e collaboratori, denominati anche incaricati o utenti, del Comune di Cittadella, indicazioni per una corretta e adeguata gestione delle informazioni comunali, in particolare attraverso l'uso di sistemi, applicazioni e strumenti informatici.

Ogni incaricato è tenuto a rispettare il presente disciplinare.

Si specifica che tutti gli strumenti utilizzati dal lavoratore, intendendo con ciò i PC, notebook, cellulari, e-mail ed altri strumenti con relativi software ed applicativi (di seguito più semplicemente "strumenti"), sono messi a disposizione dal Comune di Cittadella per rendere la prestazione lavorativa.

Gli strumenti, nonché le relative reti a cui è possibile accedere tramite gli stessi, sono domicilio informatico del Comune di Cittadella.

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 esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio comunale. Per tutela del patrimonio comunale si intende altresì la sicurezza informatica e la tutela del sistema informatico comunale. Tali informazioni sono altresì utilizzabili a tutti i fini connessi al rapporto di lavoro, visto che il presente disciplinare costituisce adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli, sempre nel rispetto di quanto disposto dal Regolamento Europeo n. 679/16 "General Data Protection".

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.

Gli Amministratori di sistema sono stati nominati con decreto del Sindaco prot. n. 49608 del 14/12/2009.

Art. 1 - Oggetto e finalità

Il presente disciplinare è redatto:

- alla luce della Legge 20.05.1970 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 n. 679/16 "General Data Protection" (d'ora in avanti Reg. n. 679/16 o GDPR);
- ai sensi del Decreto Legislativo 101/2018
- ai sensi delle "Linee guida del Garante per posta elettronica e internet" pubblicate in Gazzetta Ufficiale n. 58 del 10 marzo 2007;
- alla luce dell'art. 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 una corretta "cultura informatica" affinché l'utilizzo degli strumenti informatici e telematici forniti dal Comune sia conforme alle finalità istituzionali e nel pieno rispetto 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.

Art. 2 - Principi generali e di riservatezza nelle comunicazioni

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

- **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. n. 679/16);
- **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. Il Titolare pertanto favorisce la formazione continua di tutto il personale al fine di acquisire la necessaria consapevolezza nell'uso delle tecnologie informatiche e più in generale del corretto utilizzo dei dati personali che per motivi di lavoro si trova a trattare.
- **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 titolare dei trattamenti, i responsabili e gli autorizzati al trattamento devono 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".

È riconosciuto al Titolare del trattamento (Sindaco pro-tempore del Comune di Cittadella) il potere di svolgere attività di monitoraggio, che nella fattispecie saranno svolte dagli Amministratori di sistema o dal personale delegato dagli stessi, sempre nel rispetto della succitata normativa.

Il dipendente si attiene alle seguenti regole di trattamento dei dati:

- È vietato comunicare a soggetti non specificatamente autorizzati i dati personali comuni, categorie particolari di dati personali, dati relativi a reati e condanne penali, elementi e informazioni istituzionali dei quali viene a conoscenza nell'esercizio delle proprie funzioni e mansioni all'interno del Comune. 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.
- È vietata l'estrazione di originali e/o copie cartacee ed informatiche per uso personale di documenti, fascicoli, lettere, data base e quant'altro.
- Per le riunioni e gli incontri di particolare riservatezza si avrà cura di utilizzare sale dedicate.

Art. 3 - Tutela del lavoratore

Alla luce dell'art. 4, comma 1, L. n. 300/1970, la regolamentazione della materia indicata nell'art. 1 del presente disciplinare, 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 correttamente il sistema informativo del Comune di Cittadella per fare fronte alle esigenze produttive od organizzative e di sicurezza nel trattamento dei dati personali.

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. n. 679/16.

Art. 4 - Campo di applicazione

Il presente disciplinare si applica a tutti i dipendenti ed amministratori, senza distinzioni di ruolo e/o di livello, nonché a tutti i collaboratori dell'Ente a prescindere dal rapporto contrattuale con lo stesso intrattenuto.

Ai fini delle disposizioni dettate per l'utilizzo delle risorse informatiche e telematiche, per "utente" deve intendersi ogni dipendente, collaboratore ed amministratore in possesso di specifiche credenziali di autenticazione. Tale figura potrà anche venir indicata come "incaricato del trattamento" o "autorizzata" o "dipendente/collaboratore".

Art. 5 - Gestione, assegnazione e revoca delle credenziali di accesso

Le credenziali di autenticazione per l'accesso alle risorse informatiche vengono assegnate dagli Amministratori di sistema, previa formale richiesta del Responsabile dell'ufficio/area 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'Ufficio/area 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 e del periodo preciso di validità delle credenziali. Ogni successiva variazione delle abilitazioni di accesso ai sistemi informativi dovrà essere richiesta formalmente agli Amministratori di sistema dal Responsabile di riferimento. Dal punto di vista pratico, la richiesta consiste nella compilazione digitale del documento "Richiesta abilitazione utente", allegato al presente disciplinare in fac-simile e prelevabile in formato digitale nel percorso di rete "L:\Amministrazione digitale\Regolamento nuovi utenti", l'apposizione della firma digitale da parte del Dirigente responsabile ed invio del documento agli Amministratori di sistema.

La creazione di un nuovo utente di dominio sarà presa in considerazione solo per collaboratori il cui periodo di permanenza sia stimato maggiore di n. 2 mesi. In caso contrario, il nuovo collaboratore potrà essere di affiancamento al personale autorizzato e non potrà accedere al sistema informatico comunale con proprie credenziali e ruoli autorizzativi.

Le credenziali di autenticazione consistono in un codice per l'identificazione dell'utente (altresì nominati username, nome utente o user id), 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.

La password deve essere di adeguata robustezza: deve essere composta da almeno 8 caratteri, formata da lettere maiuscole e minuscole e/o numeri e caratteri speciali. Non deve contenere riferimenti agevolmente riconducibili all'utente (username, nomi o date relative alla persona o ad un famigliare).

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 categorie particolari di dati personali, è obbligatorio il cambio password almeno ogni tre mesi. Tali utenti saranno individuati mediante l'indicazione riportata sul Registro dei trattamenti (art. 30 del Reg. n. 679/16).

Nel caso di cessazione del rapporto di lavoro con il dipendente/collaboratore, il Responsabile dell'Ufficio/area di riferimento, dovrà comunicare formalmente e preventivamente all'Amministratore di sistema la data effettiva a partire dalla quale le credenziali saranno disabilitate.

Art. 6 - Utilizzo della rete del Comune di Cittadella

Per l'accesso alle risorse informatiche del Comune di Cittadella attraverso la rete locale, ciascun incaricato deve essere in possesso di credenziali di autenticazione secondo l'art. 5 "Gestione, assegnazione e revoca delle credenziali di accesso".

È assolutamente proibito accedere alla rete e nei sistemi informativi utilizzando credenziali di altre persone.

L'accesso alla rete garantisce a ciascun autorizzato la disponibilità di condivisioni di rete (cartelle su server) nelle quali vanno inseriti e salvati i files di lavoro, organizzati per area/ufficio o per diversi criteri o per obiettivi specifici di lavoro.

L'organizzazione e la gestione dell'albero delle sottocartelle è demandata al Referente informatico di settore di cui al successivo art. 13. Questi ha anche il compito di effettuare una pulizia periodica degli archivi, con cancellazione dei file obsoleti, duplicati o inutili. Nel caso di un'organizzazione di settore distribuita, il referente informatico ha il compito di monitorare che la suddetta buona pratica venga messa in atto.

Ciascun incaricato poi, dispone di un'area riservata e personale nel server comunale. Tutte le cartelle di rete, siano esse condivise o personali, possono ospitare esclusivamente contenuti professionali. Pertanto è vietato il salvataggio sui server del Comune, 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 dagli Amministratori di sistema o dal personale delegato dagli stessi, a seguito di interventi di sicurezza informatica ovvero di manutenzione/aggiornamento su server ed anche sugli strumenti viene rimosso, ferma ogni ulteriore responsabilità civile, penale e disciplinare.

Con regolare periodicità (almeno una volta al mese), ciascun utente autorizzato provvede alla pulizia degli archivi dell'area personale, con cancellazione dei file obsoleti o inutili. Particolare attenzione deve essere prestata alla duplicazione dei dati, essendo infatti necessario evitare un'archiviazione ridondante.

Tutte le risorse di memorizzazione, diverse da quelle citate precedentemente, non sono sottoposte al controllo regolare degli Amministratori 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", "Download" 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, poiché non sono garantite la sicurezza e la protezione contro l'eventuale perdita.

Senza il consenso del Titolare, è vietato trasferire documenti elettronici dai sistemi informativi e strumenti del Comune a device esterni (hard disk, chiavette, CD, DVD e altri supporti).

Senza il consenso del Titolare è vietato salvare documenti elettronici del Comune (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.

I log relativi all'utilizzo di strumenti, reperibili nella memoria degli stessi ovvero sui server nonché i file con essi trattati sono registrati e possono essere oggetto di controllo da parte del Titolare del trattamento, per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio comunale.

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

Art. 7 - Utilizzo degli strumenti elettronici

(PC, notebook ed altri strumenti e relativi software di sistema ed applicativi)

L'incaricato è consapevole che gli strumenti forniti sono di proprietà del Comune di Cittadella e che 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 incaricato si deve quindi attenere alle seguenti regole di utilizzo degli strumenti:

- L'accesso agli strumenti messi a disposizione del Comune è protetto da password; per l'accesso devono essere utilizzati username e password assegnate dagli Amministratori di sistema così come disciplinato dall'art. 5 del presente disciplinare. A tal proposito si rammenta che essi sono strettamente personali e ciascun incaricato è tenuto a conservarli nella massima segretezza.
- 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 agli Amministratori di sistema ogni malfunzionamento e/o danneggiamento. Non è consentita l'attivazione della password d'accensione (BIOS).
- Non è consentito modificare le configurazioni hardware e software impostate dagli Amministratori di sistema sugli strumenti assegnati.
- Tutto il software in uso nel sistema informativo del Comune di Cittadella, deve essere ottenuto seguendo le procedure e le linee guida dell'Ente e deve essere registrato a nome dell'Amministrazione Comunale. Tutto il personale è tenuto al rispetto delle leggi in materia di tutela della proprietà intellettuale (copyright) e non può installare, duplicare od utilizzare qualsiasi tipologia di software al di fuori di quanto consentito dagli accordi di licenza.
- Al fine di proteggere l'integrità del sistema informativo del Comune di Cittadella, il personale non può utilizzare eventuale hardware o software di proprietà personale. Tutto ciò comprende anche le applicazioni regolarmente acquistate e registrate, programmi shareware e/o freeware, eventuale software scaricato da internet o proveniente da CD/DVD allegati a riviste o altro software posseduto a qualsiasi titolo.
- Ciascun incaricato è tenuto a scollegarsi dal sistema, o bloccare l'accesso, ogni qualvolta sia

costretto ad assentarsi dal locale nel quale è ubicata la stazione di lavoro (PC) o nel caso ritenga di non essere in grado di presidiare l'accesso alla medesima. Il PC incustodito, connesso alla rete, può essere utilizzato da parte di terzi, senza che vi sia la possibilità di provarne in seguito l'indebito uso.

- La gestione dei dati su PC è demandata a ciascun incaricato, che dovrà provvedere a memorizzare sulle condivisioni comunali i dati che possono essere utilizzati anche da altri utenti, evitando di mantenere l'esclusività su di essi.
- Gli Amministratori di sistema possono in qualunque momento procedere alla rimozione di ogni file o applicazione che riterrà essere pericolosi per la sicurezza del sistema informativo, nonché tutte le impostazioni eventualmente configurate che possano interferire con il corretto funzionamento dei servizi informatici comunali.
- 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.
- È vietato utilizzare il PC per l'acquisizione, la duplicazione e/o la trasmissione illegale di opere protette da copyright.
- È vietato l'utilizzo di supporti di memoria (chiavi USB, CD, DVD o altri supporti) per il salvataggio di dati trattati tramite gli strumenti comunali, salvo che il supporto utilizzato sia stato fornito dagli Amministratori di sistema. In tale caso, il supporto fornito può essere utilizzato esclusivamente per finalità lavorative e non può essere connesso a strumenti diversi da quelli comunali.
- È assolutamente vietato connettere al PC qualsiasi periferica (compresi i cellulari o smartphone per operazioni di ricarica o trasferimento file) non autorizzata preventivamente dagli Amministratori di sistema.
- È assolutamente vietato connettere alla rete locale qualsiasi dispositivo (PC esterni, router, switch, modem, etc.) non autorizzato preventivamente dagli Amministratori di sistema.
- Nel caso in cui l'incaricato dovesse notare comportamenti anomali del PC, è tenuto a comunicarlo tempestivamente agli Amministratori di sistema.

I log relativi all'utilizzo di strumenti, reperibili nella memoria degli strumenti stessi ovvero sui Server o sui router comunali, nonché i file con essi trattati sono registrati e possono essere oggetto di controllo da parte del Titolare del trattamento, attraverso gli Amministratori di sistema, per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio comunale.

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

Art. 8 - Utilizzo di internet

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

L'utilizzo di internet deve essere limitato a scopi inerenti l'attività lavorativa.

Il Titolare si riserva di applicare profili di navigazione personalizzati per gruppi di utenti o per settori, a seconda dell'attività professionale svolta.

Ciascun incaricato si deve attenere alle seguenti regole di utilizzo della rete internet e dei relativi

servizi:

- È ammessa solo la navigazione in siti considerati correlati con la prestazione lavorativa. L'accesso è consentito dal proxy comunale con le sue policy di sicurezza debitamente implementate e aggiornate, ad es. i siti istituzionali, i siti degli Enti locali, di fornitori e partner istituzionali.
- È vietato compiere azioni che siano potenzialmente in grado di arrecare danno al Comune, 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.
- È vietato a chiunque il download di qualunque tipo di software gratuito (freeware) o shareware prelevato da siti internet, se non espressamente autorizzato dagli Amministratori di sistema.
- Il Titolare si riserva di bloccare l'accesso a siti "a rischio" 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. In caso di blocco accidentale di siti di interesse comunale, contattare gli Amministratori di sistema per uno sblocco selettivo.
- Nel caso in cui, per ragioni di servizio, si necessiti di una navigazione libera dai filtri del suddetto proxy, è necessario richiedere lo sblocco mediante una mail indirizzata agli Amministratori di sistema, ed in copia al Titolare, 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. Ciascun incaricato, nello svolgimento delle proprie attività, deve comunque tenere presente in modo particolare le indicazioni contenute nel presente disciplinare.
- È tassativamente 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 dagli Amministratori di sistema, con il rispetto delle normali procedure di acquisto.
- È assolutamente vietato l'utilizzo di abbonamenti privati per effettuare la connessione ad internet, tranne in casi del tutto eccezionali e previo parere ed autorizzazione degli Amministratori di sistema.
- È assolutamente 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).
- 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 la 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 dipendenti/collaboratori.

Al fine delle verifiche di cui al presente disciplinare, si informa che il Comune, per il tramite degli Amministratori di sistema, 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, il Titolare, per tramite del Responsabile esterno incaricato, può conservare 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. La conservazione non può essere superiore a giorni trenta.

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

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

Art. 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 incaricato si deve attenere alle seguenti regole di utilizzo dell'indirizzo di posta elettronica:

- Ad ogni utente viene fornito un account e-mail nominativo ed il suo utilizzo deve essere limitato esclusivamente allo scopo di rendere la propria prestazione lavorativa. E' assolutamente vietato ogni utilizzo di tipo privato. L'utente a cui è assegnata una casella di posta elettronica, è responsabile del corretto utilizzo della stessa.
- Il Comune fornisce, altresì, delle caselle di posta elettronica associate a ciascuna unità organizzativa, ufficio o gruppo di lavoro 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 comunali.
- L'iscrizione a mailing-list o newsletter esterne con il proprio indirizzo comunale personale è concessa esclusivamente per motivi professionali. Prima di iscriversi occorre verificare anticipatamente l'affidabilità del sito che offre il servizio.
- Allo scopo di garantire sicurezza alla rete, 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. E' 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 gli Amministratori di sistema per una valutazione dei singoli casi.
- Non é consentito diffondere messaggi del tipo "catena di S. Antonio" o simili, anche se il contenuto sembra meritevole di attenzione. In generale è vietato l'invio di messaggi pubblicitari di qualsiasi tipo.
- Nel caso fosse necessario inviare allegati "pesanti" (fino a 20 MB) 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 rivolgersi agli Amministratori di sistema per l'utilizzo di programmi specialistici di file transfer basati su tecnologia web.
- Nel caso in cui fosse necessario inviare a destinatari esterni messaggi contenenti allegati con dati

personali sensibili, è obbligatorio che questi allegati vengano preventivamente resi inintelligibili attraverso crittazione 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 istituzionali, i dati personali e/o sensibili di competenza comunale possono essere inviati soltanto a destinatari - persone o Enti – qualificati e competenti già individuati nell'apposito Registro dei trattamenti.

- Non è consentito l'invio automatico di e-mail del Comune all'indirizzo e-mail privato (attivando per esempio un "inoltro" automatico delle e-mail entranti), anche durante i periodi di assenza (es. ferie, malattia, infortunio ecc.). In questa ultima ipotesi, è raccomandabile utilizzare un messaggio di "Assenza ufficio" facendo menzione di chi, all'interno del Comune, assumerà le mansioni durante l'assenza, oppure indicando un indirizzo di mail alternativo preferibilmente di tipo collettivo, tipo ufficio-xxx@comune.cittadella.pd.it. Rivolgersi agli Amministratori di sistema per tale eventualità.
- In caso di assenza improvvisa o prolungata e per improrogabili necessità legate all'attività lavorativa, qualora non fosse possibile attivare la funzione "risposta automatica" o l'inoltro automatico su altre caselle di posta del Comune 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 quelli ritenuti rilevanti per lo svolgimento dell'attività lavorativa. Sarà compito del Responsabile di Area assicurarsi che sia redatto un verbale attestante quanto avvenuto.
- La diffusione massiva di messaggi di posta elettronica deve essere effettuata esclusivamente per motivi inerenti il servizio, possibilmente su autorizzazione del Responsabile di Area 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.
- È vietato inviare posta elettronica in nome e per conto di un altro utente, salvo sua espressa autorizzazione anche verbale.
- È vietato inviare posta elettronica ad un elevato numero di destinatari interni (> 10) con allegati. Nelle comunicazioni interne, in generale, è sempre preferibile depositare l'allegato nelle cartelle condivise della rete interna e fare riferimento al link nella mail.
- In caso di necessità di invio di allegati, è sempre necessario controllare il peso degli stessi e, nel caso di foto e video, di procedere preventivamente alla loro riduzione in termini di peso mediante l'utilizzo di appositi programmi forniti su richiesta dagli Amministratori di sistema.
- La casella di posta elettronica personale deve essere mantenuta in ordine, cancellando messaggi e documenti la cui conservazione non è più necessaria. Anche la conservazione di messaggi con allegati pesanti è da evitare per quanto possibile, preferendo, in alternativa, il salvataggio dell'allegato sulle condivisioni comunali.
- 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 ed il mittente/destinatario viene avvisato mediante messaggio specifico. Ne consegue che è assolutamente vietato ricevere messaggi e file allegati attraverso canali diversi da quelli messi a disposizione dagli Amministratori di sistema in quanto non opportunamente analizzati. Più esplicitamente, è ammessa la ricezione di messaggi ed allegati solo dalla mail istituzionale ed è vietato l'accesso e l'utilizzo delle mail private (gmail, libero, tiscali ecc..) e di altri strumenti di condivisione (whatsapp, istagram, facebook ecc..).

Si informa che, ai sensi dell'art. 2214 del Codice civile e dell'articolo 22 del D.P.R. n. 600/73, il Titolare deve conservare per dieci anni sui propri server di posta elettronica tutti i messaggi di posta elettronica a contenuto e rilevanza giuridica e commerciale provenienti da e diretti a domini istituzionali e/o comunali.

Si informa altresì che il Titolare, per il tramite degli Amministratori di sistema, 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 ovvero per motivi di sicurezza del sistema informatico, il Titolare per il tramite degli Amministratori di sistema può accedere all'account di posta elettronica istituzionale, prendendo visione dei messaggi, salvando o cancellando file.

Si informa che, in caso di cessazione del rapporto lavorativo, la mail comunale affidata all'incaricato verrà sospesa per un periodo di 6 mesi e successivamente disattivata. Nel periodo di sospensione il sistema genera una risposta automatica al mittente, invitandolo a rispedire il messaggio ad altro indirizzo mail comunale.

Art. 10 - Utilizzo dei telefoni, fax, fotocopiatori, scanner e stampanti

Il dipendente è consapevole che gli strumenti di stampa, di scansione, il telefono, sono di proprietà del Comune di Cittadella e sono resi disponibili al dipendente/collaboratore per rendere la prestazione lavorativa. Pertanto ne viene concesso l'uso esclusivamente per tale fine.

Il telefono comunale affidato al dipendente/collaboratore 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 consentito solo nel caso di comprovata necessità ed urgenza con conseguente rimborso delle spese all'Ente.

L'assegnazione di un telefono cellulare e relativa sim dovrà essere richiesta formalmente agli Amministratori di sistema dal Responsabile del servizio di riferimento.

Il personale preposto provvederà a consegnare gli strumenti opportunamente configurati in base alle esigenze di servizio ed alla compilazione del documento "Modulo assegnazione scheda sim e cellulare", allegato al presente disciplinare in fac-simile, e richiederà all'assegnatario la controfirma per avvenuta ricezione e conoscenza del presente disciplinare.

Qualora venisse assegnato un cellulare istituzionale all'utente, quest'ultimo sarà responsabile del suo utilizzo e della sua custodia. Ai cellulari, smartphone e tablet comunali si applicano le medesime regole sopra previste per gli altri dispositivi informatici, 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 (vedi art. 8), se consentita.

Ciascun dipendente/collaboratore si deve attenere alle seguenti regole di utilizzo:

- Per gli smartphone e tablet comunali è vietata l'installazione e l'utilizzo di applicazioni (o altresì denominate "app" nel contesto degli smartphone) diverse da quelle autorizzate dagli Amministratori di sistema.
- È vietato l'utilizzo delle fotocopiatrici comunali per fini personali, salvo preventiva ed esplicita autorizzazione da parte del Responsabile di Area.
- Per quanto concerne l'uso delle stampanti gli utenti sono tenuti a:
    a. Stampare documenti **solo se strettamente necessari** per lo svolgimento delle proprie funzioni operative

b. Prediligere le stampanti di rete condivise, rispetto a quelle locali/personali, per ridurre l'utilizzo di materiali di consumo (toner ed altri consumabili)
c. Prediligere la stampa in bianco/nero e fronte/retro al fine di ridurre i costi, se possibile.

- Nel caso in cui si rendesse necessaria la stampa di informazioni riservate l'utente dovrà presidiare il dispositivo di stampa per evitare la possibile perdita o divulgazione di tali informazioni e persone terze non autorizzate.

Art. 11 - Assistenza agli utenti e manutenzioni

Gli Amministratori di sistema, in base alla tipologia dell'intervento richiesto, possono accedere ai dispositivi informatici comunali sia direttamente, sia mediante software di accesso remoto, per i seguenti scopi:

- verifica e risoluzione di problemi sistemistici ed applicativi, su segnalazione dell'utente finale.
- verifica del corretto funzionamento dei singoli dispositivi in caso di problemi rilevati nella rete.
- richieste di aggiornamento software e manutenzione preventiva hardware e software.

Gli interventi tecnici posso avvenire previo consenso del dipendente/collaboratore, 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 del dipendente/collaboratore cui la risorsa è assegnata.

L'accesso in teleassistenza sui PC della rete comunale richiesto da terzi (fornitori e/o altri opportunamente nominati Responsabili esterni al trattamento dei dati dal Responsabile di area) deve essere autorizzato dagli Amministratori 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.

Durante gli interventi in teleassistenza da parte di operatori terzi, l'utente richiedente o gli Amministratori di sistema devono presenziare la sessione remota, in modo tale da verificare ed impedire eventuali comportamenti non conformi al presente disciplinare.

Art. 12 - Acquisto di hardware e software

Per prevenire l'introduzione di virus e/o altri programmi dannosi e per proteggere l'integrità del sistema informativo del Comune di Cittadella, tutto l'hardware ed il software in dotazione agli uffici deve essere assegnato dagli Amministratori di sistema, in quanto competenti in materia.

In caso di necessità di acquisto o dotazione di software applicativi e/o procedure pertinenti alle varie aree gestionali del Comune, la cui procedura di acquisto, per competenza di materia, sarà a cura del relativo Responsabile di area, deve essere richiesta la consulenza e l'autorizzazione preventiva al Responsabile dell'Ufficio Servizi informativi, innovazione tecnologica, C.E.D. al fine di garantire la compatibilità funzionale e tecnica ed il mantenimento dell'efficienza operativa dei sistemi e delle reti.

Ogni acquisto di carattere informatico effettuato da Servizi diversi da quello informatico, dovrà avvenire con determinazioni redatte attraverso il modello "Determina di carattere informatico" che prevede, nel suo flusso formativo, l'apposizione del visto del Responsabile dell'Ufficio Servizi informativi, innovazione tecnologica, C.E.D..

La stipula dei contratti successivi di manutenzione ed assistenza possono avvenire a cura del personale dell'Ufficio Servizi informativi, innovazione tecnologica, C.E.D., previa richiesta scritta del Responsabile di riferimento ed attestazione annuale di volontà a mantenere per ragioni organizzative e di servizio il software/hardware in uso.

Art. 13 - Referente informatico di settore

Ciascun Responsabile designerà un referente informatico. Nel caso di strutture complesse potranno essere nominati più referenti informatici in accordo con gli Amministratori di sistema.

Al Referente saranno assegnati i seguenti compiti:

- Verificare le esigenze di strumentazione informatica e segnalarle al responsabile dell'Ufficio Servizi informativi, innovazione tecnologica, C.E.D..
- Collaborare con gli Amministratori di sistema nella supervisione sul corretto utilizzo delle risorse informatiche;
- Assolvere a quanto previsto nell'art. 6 par. 4 – "*Utilizzo della rete del Comune di Cittadella*" del presente disciplinare.
- Collabora con il Responsabile dell'ufficio Servizi informativi, innovazione tecnologica, C.E.D. nella promozione ed attuazione di progetti informatici di carattere "trasversale" nell'Ente.

I referenti dovranno avere conoscenze idonee al ruolo.

Art. 14 - Conservazione dei dati

In riferimento agli articoli 5 e 6 del Reg. n. 679/16 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 dodici mesi dalla loro produzione.

In casi eccezionali – ad esempio: per 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 – è consentito il prolungamento dei tempi di conservazione limitatamente al soddisfacimento delle esigenze sopra esplicitate.

Il Titolare 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.

Art. 15 - Partecipazioni a Social Media

L'utilizzo a fini promozionali e commerciali di Facebook, Twitter, Linkedin, dei blog e dei forum, anche professionali (ed altri siti o social media) è gestito ed organizzato esclusivamente dal Titolare attraverso specifiche direttive ed istruzioni operative al personale a ciò espressamente addetto, rimanendo escluse iniziative individuali da parte dei singoli dipendenti/collaboratori.

Fermo restando il diritto della persona alla libertà di espressione, il Comune ritiene comunque opportuno indicare ai dipendenti/collaboratori alcune regole comportamentali, al fine di tutelare tanto la propria immagine ed il patrimonio, anche immateriale, quanto i propri collaboratori, i propri clienti e fornitori, gli altri partners, oltre che gli stessi dipendenti/collaboratori utilizzatori dei social media, fermo restando che è vietata la partecipazione agli stessi social media durante l'orario di lavoro.

Il presente articolo deve essere osservato dai dipendenti/collaboratori sia che utilizzino dispositivi messi a disposizione dal Comune, sia che utilizzino propri dispositivi, sia che partecipino ai social media a titolo personale, sia che lo facciano per finalità professionali, come dipendenti/collaboratori del Comune.

La condivisione dei contenuti nei social media deve sempre rispettare e garantire la segretezza sulle informazioni istituzionali considerate dal Titolare riservate ed in genere, a titolo esemplificativo e non esaustivo, sulle informazioni inerenti attività, dati contabili, finanziari, progetti, procedimenti svolti o

in svolgimento presso gli uffici. Inoltre, ogni comunicazione e divulgazione di contenuti dovrà essere effettuata nel pieno rispetto dei diritti di proprietà industriale e dei diritti d'autore, sia di terzi che del Comune. Il dipendente/collaboratore, nelle proprie comunicazioni, non potrà quindi inserire il nominativo e il logo del Comune, né potrà pubblicare disegni, modelli od altro connesso ai citati diritti. Ogni deroga a quanto sopra disposto potrà peraltro avvenire solo previa specifica autorizzazione del Titolare.

Il dipendente/collaboratore deve garantire la tutela della riservatezza e dignità delle persone; di conseguenza, non potrà comunicare o diffondere dati personali (quali dati anagrafici, immagini, video, suoni e voci) di colleghi e in genere di collaboratori comunali, se non con il preventivo personale consenso di questi, e comunque non potrà postare nei social media immagini, video, suoni e voci registrati all'interno dei luoghi di lavoro, se non con il preventivo consenso del Titolare.

Art. 16 - Controlli sugli strumenti

(art. 6.1 Provv. Garante - Del. n. 13 del 1° marzo 2007, ad integrazione dell'Informativa ex art. 13 Reg. n. 679/16)

Poiché in caso di violazioni contrattuali e giuridiche, sia il Titolare, sia il singolo lavoratore sono potenzialmente perseguibili con sanzioni, anche di natura penale, il Titolare verificherà, nei limiti consentiti dalle norme legali e contrattuali, il rispetto delle regole e l'integrità del proprio sistema informatico. Il datore di lavoro, infatti, può avvalersi legittimamente, nel rispetto dello Statuto dei lavoratori (art. 4, comma 2), di sistemi che consentano indirettamente il controllo a distanza (c.d. controllo preterintenzionale) e determinino un trattamento di dati personali riferiti o riferibili ai lavoratori. 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. I controlli devono essere effettuati nel rispetto del presente disciplinare. E' riconosciuto al Titolare il potere di svolgere attività di monitoraggio, che nella fattispecie saranno svolte solo dagli Amministratori di Sistema o dal personale da essi delegato, sempre nel rispetto della succitata normativa e del presente disciplinare 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 disciplinare ha l'obiettivo di informare i dipendenti/collaboratori 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.

L'uso degli strumenti informatici del Comune può lasciare traccia delle informazioni sul relativo uso, come analiticamente spiegato nei riquadri di cui ai punti 6 – 7 – 8 – 9 del presente disciplinare. Tali informazioni, che possono contenere dati personali eventualmente anche sensibili del dipendente/collaboratore, possono essere oggetto di controlli da parte del Titolare, per il tramite degli Amministratori di Sistema, volti a garantire esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio, nonché per la sicurezza e la salvaguardia del sistema informatico e 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 16.1 e 16.2) e possono permettere al Titolare di prendere indirettamente cognizione dell'attività svolta con gli strumenti.

1. Controlli per la tutela del patrimonio, 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 agli articoli 6 – 7 – 8 – 9, il Titolare del trattamento dei dati personali per il tramite degli Amministratori di Sistema, si atterrà al processo descritto qui di seguito (se e in quanto compatibile con lo Strumento oggetto di controllo).

a. 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 disciplinare.
b. Successivamente, dopo almeno 7 giorni, se il comportamento anomalo persiste, il Titolare potrà autorizzare il personale addetto al controllo, potendo così accedere alle informazioni descritte negli articoli 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.
c. Qualora il rischio di compromissione del sistema informativo aziendale sia imminente e grave a tal punto da non permettere l'attesa dei tempi necessari per i passaggi procedimentali descritti negli articoli 1 e 2, il Responsabile del Trattamento, unitamente all'Amministratore di sistema, può intervenire senza indugio sullo strumento da cui proviene la potenziale minaccia.

2. 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 dipendente/collaboratore (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 agli articoli 6 – 7 – 8 – 9 il Responsabile del trattamento dei dati personali, per il tramite degli Amministratori di Sistema, si atterrà alla procedura descritta qui di seguito (se e in quanto compatibile con lo Strumento oggetto di controllo).
   a. Redazione di un atto da parte del Titolare del trattamento che comprovi le necessità produttive e di organizzazione che richiedano l'accesso allo strumento.
   b. Incarico agli Amministratori di sistema di accedere alla risorsa con credenziali di Amministratore ovvero tramite l'azzeramento e la contestuale creazione di nuove credenziali di autenticazione del dipendente/collaboratore interessato, con avviso che al primo accesso alla risorsa, lo stesso dovrà inserire nuove credenziali.
   c. Redazione di un verbale che riassuma i passaggi precedenti.
   d. In ogni caso l'accesso ai documenti presenti nella risorsa è limitato a quanto strettamente indispensabile alle finalità produttive e di organizzazione del lavoro.
   e. 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 disciplinare costituisce adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli, sempre nel rispetto di quanto disposto dal Regolamento Europeo n. 679/16 "General Data Protection".

Art. 17 - Sanzioni disciplinari

È fatto obbligo a tutti i dipendenti/collaboratori di osservare le disposizioni portate a conoscenza con il presente disciplinare. Eventuali violazioni del presente disciplinare nonché di altre norme previste dal CCRL applicato, a seconda della gravità dell'infrazione, comportano l'adozione dei seguenti provvedimenti:

- Richiamo scritto;
- Multa;
- Licenziamento con preavviso;

Rimane comunque riservato il diritto di intraprendere azioni civili e penali nei confronti dei responsabili di qualsivoglia violazione a danno del Comune.

Art. 18 - Disposizioni finali

Il presente disciplinare è stato redatto dal Responsabile Ufficio Servizi informativi, innovazione tecnologica, C.E.D. (sentiti il Dirigente competente ed il Segretario Generale) che è chiamato a garantire il coordinamento degli adempimenti.

La sua pubblicizzazione, avverrà nelle seguenti forme:

- trasmissione per posta elettronica interna a tutti i TPO e a tutti i dipendenti/collaboratori provvisti di e-mail istituzionale;
- mediante pubblicazione sulla sezione Amministrazione trasparente - sezione Disposizioni Generali - sotto sezione Atti generali.
- in allegato alla lettera di incarico al trattamento dati ai sensi Reg. n. 679/16.

Tutti i dipendenti/collaboratori possono proporre, quando ritenuto necessario, integrazioni e modifiche al presente disciplinare tramite comunicazione scritta al Responsabile Ufficio Servizi informativi, innovazione tecnologica, C.E.D..

Legenda

Amministratore di sistema - E' il gestore di una rete (LAN), solitamente connessa ad Internet. Alcune operazioni effettuate dall'amministratore sono: * verifica del corretto funzionamento della rete locale; * ricambio delle schede di rete; * installazione programmi; * gestione delle pagine web;* gestione dell'e-mail degli user, delle newsgroup, ecc.; * limitazione dei diritti di accesso ai file(directory comprese); * definisce quali operazioni possono essere eseguite dagli utenti, la quota(massimo spazio disponibile per memorizzare nell'unità di massa i file dell'utente); * effettuare ogni tipo di operazione su qualsiasi risorsa degli utenti grazie all'accesso root; * suggerire la risoluzione dei problemi più comuni, relativi alla connessione e al regolare funzionamento del sistema.

BIOS – Software di basso livello che fornisce ad un PC le funzioni di base per l'accesso all'hardware. E' il primo programma eseguito all'accensione, prima ancora del sistema operativo.

Chat line - Il termine chat (in inglese, letteralmente, "chiacchierata"), viene usato per riferirsi a un'ampia gamma di servizi sia telefonici che via Internet; ovvero, complessivamente, quelli che i paesi di lingua inglese distinguono di solito con l'espressione "online chat", "chat in linea". Questi servizi, anche piuttosto diversi fra loro, hanno tutti in comune due elementi fondamentali: il fatto che il dialogo avvenga in tempo reale, e il fatto che il servizio possa mettere facilmente in contatto perfetti sconosciuti, generalmente in forma essenzialmente anonima. Il "luogo" (lo spazio virtuale) in cui la chat si svolge è chiamato solitamente chatroom (letteralmente "stanza delle chiacchierate"), detto anche channel (in italiano canale), spesso abbreviato chan.

Download o upload - In generale con questo termine si intende il trasferimento di dati da un computer locale a uno remoto utilizzando un apparato di comunicazione, ad es. il modem, o tra computer della stessa rete Per download si intende anche la visualizzazione sul proprio computer di una pagina internet.

Freeware - Software gratuito realizzato e distribuito da privati o piccole società,attraverso Internet o CD- ROM allegati a pubblicazioni in edicola.

Forum – struttura informatica che consente la discussione online, tramite internet, degli utenti. Utilizzato per la discussione su temi specifici.

Guest book - Fornisce ai visitatori l'opportunità di lasciare commenti (sul sito) per i nuovi utenti che entreranno nel sito

Mailing list – Sistema organizzato per la partecipazione di più persone in una discussione asincrona mediante e-mail.

Malware – Software creato con l'intento di causare danni ad un sistema informatico o di carpire dati personali memorizzati in un sistema informatico.

Newsletter – notiziario scritto diffuso tramite e-mail agli utenti iscritti.

Phishing – attività illegale che sfrutta messaggi di posta elettronica ingannevoli per ottenere l'accesso a informazioni personale anche di carattere riservato, con la finalità del furto di identità nell'ambito di comunicazioni elettroniche. Utenti truffatori inviano messaggi che imitano logo e grafica di siti istituzionali con richieste di inserimento di dati personali, come numeri di carta di credito, codici personali e segreti di accesso etc. Si possono individuare da un attento esame del contenuto del messaggio che spesso contengono collegamenti a siti non istituzionali.

Proxy - Un proxy è un programma che si interpone tra un client ed un server, inoltrando le richieste e le risposte dall'uno all'altro. Il client si collega al proxy invece che al server, e gli invia delle richieste. Il proxy a sua volta si collega al server e inoltra la richiesta del client, riceve la risposta e la inoltra al client. In informatica, con client (in italiano detto anche cliente) si indica una componente che accede ai servizi o alle risorse di un'altra componente, detta server. In questo contesto si può quindi parlare di client riferendosi all'hardware o al software.

Remote banking - Per remote banking si intende l'insieme di servizi automatizzati che permettono ai clienti, grazie all'uso di terminali o di un semplice telefono, di collegarsi alla banca presso la quale intrattengono il conto corrente ed effettuare una serie di operazioni bancarie oppure di ricevere informazioni in tempo reale. A seconda del mezzo di comunicazione utilizzato si può parlare di phone banking ed internet banking.

Shareware - Software messo a disposizione su una rete o su CD/DVD e acquistabile a basso prezzo dopo un periodo di prova gratuita.

Social network – servizio online che consiste nella connessione di persone legate da diversi legami sociali, quali interessi comuni, rapporti di lavoro, legami affettivi fino alla conoscenza casuale.

Spam – messaggi di posta elettronica non sollecitati con contenuto generalmente commerciale.

***.exe, *.com, *.vbs, *.htm, *.scr, *.bat, *.js e *.pif** - Si tratta di estensioni di file che mandano in esecuzione file eseguibili che, a loro volta, possono infettare il computer con un virus.

Richiesta di abilitazione all'accesso al sistema informatico del COMUNE di CITTADELLA.

Il/la sottoscritto/a _____ in qualità di Responsabile Area N. _____

CHIEDE

che il seguente soggetto:

Nome e Cognome: _____

Codice Fiscale: _____ Data di Nascita: _____

Ufficio di Assegnazione: _____

Tipo di rapporto con l'ente: _____

Data Inizio Servizio: _____ Data Fine Servizio: _____

venga abilitato all'accesso al sistema informatico del comune di Cittadella come di seguito specificato:

Accesso ad Internet	☐ Sì ☐ No	Accesso cartelle dell'ufficio sul server (Z:)	☐ Sì ☐ No
E-mail nominativa "nome.cognome@" (facoltativa solo per i non dipendenti)	☐ Sì ☐ No	Accesso cartelle delll'ente sul server (L:)	☐ Sì ☐ No
Accesso e-mail dell'ufficio	☐ Sì ☐ No	Rilascio badge per ril. presenze Abilitazione apertura porte	☐ Sì ☐ No ☐ Sì ☐ No
Procedure informatiche - (il SI abilita anche alla modifica. Per i lavoratori temporanei, le procedure legate alla struttura organizzativa dell'Ente (SO) non possono essere selezionate e la procedura Demografici può essere abilitata in sola consultazione tramite il portale web)			
Demografici	☐ Sì ☐ No ☐ Consultazione	LLPP	☐ Sì ☐ No ☐ Consultazione
Contabilità Finanziaria (SO)	☐ Sì ☐ No ☐ Consultazione	Edilizia Privata	☐ Sì ☐ No ☐ Consultazione
Tributi	☐ Sì ☐ No ☐ Consultazione	Gestione Atti (SO)	☐ Sì ☐ No ☐ Consultazione
Cassa Economale	☐ Sì ☐ No ☐ Consultazione	Protocollo (SO)	☐ Sì ☐ No ☐ Consultazione
Personale (SO)	☐ Sì ☐ No ☐ Consultazione	Contravvenzioni	☐ Sì ☐ No ☐ Consultazione
Altre Procedure (specifiche per ufficio/area):			
	☐ Sì ☐ No ☐ Consultazione		☐ Sì ☐ No ☐ Consultazione

	☐ Sì ☐ No ☐ Consultazione		☐ Sì ☐ No ☐ Consultazione

Altre richieste/note:

Il/la sottoscritto/a certifica con la presente, che il soggetto sopra indicato è in possesso dei requisiti legali per l'accesso al sistema informatico e ai dati in esso contenuti e che è già stato incaricato e autorizzato al trattamento dei dati personali e sensibili con cui potrà venire in contatto per ragioni di servizio ai sensi della vigente normativa.

Data di compilazione:

Firmato digitalmente da

MODULO ASSEGNAZIONE SCHEDA SIM E TELEFONO CELLULARE.

Vista la richiesta del Dirigente del Settore/Amministratore _____ inoltrata in data _____, inerente alla richiesta di utilizzo di una SIM e di telefono cellulare per motivate esigenze di servizio.

SI ASSEGNA

Al Sig._____, Amministratore/Dipendente del Comune di Cittadella, Settore e Servizio_____, l'utilizzo della seguente apparecchiatura di rete mobile comunale:

Utenza SIM:

N._____, Codice Scheda:_____

Telefono cellulare GSM/Satellitare

- Marca _____
- Modello _____
- Numero Seriale _____
- Codice IMEI _____
- Caricatore per batteria _____
- Auricolare _____
- Altro _____

Cittadella, lì

L' Amministratore di Sistema

_____

Per Ricevuta, l'utilizzatore

L'utilizzatore si impegna a garantire il corretto impiego dell'apparecchiatura di rete mobile assegnata, per gli usi e nelle modalità consentite dal "Disciplinare per l'utilizzo delle risorse informatiche e telefoniche del Comune di Cittadella", di cui ne ha preso conoscenza, ricevendone copia o reperendolo al link: L:\Amministrazione digitale\Disciplinare utilizzo strumenti informatici e telefonici.

L'utilizzatore dichiara altresì di conoscere ed accettare espressamente ed integralmente per iscritto quanto segue:

- di essere perfettamente edotta/o circa le modalità di funzionamento del materiale assegnato;
- di assumere diretta responsabilità per il suo danneggiamento, smarrimento o furto causati da sua comprovata colpa e di riconsegnare quanto assegnato in qualsiasi momento a seguito di semplice richiesta dell'Amministratore di Sistema.

Data _____	Per Ricevuta, l'utilizzatore

COMUNE DI CITTADELLA

Cittadella Città d'Arte

PROVINCIA DI PADOVA

Proposta N. 2019 / 1379
SERVIZIO CED

OGGETTO: APPROVAZIONE REGOLAMENTO PER L'UTILIZZO DELLE RISORSE INFORMATICHE E TELEFONICHE DEL COMUNE DI CITTADELLA.

PARERE IN ORDINE ALLA REGOLARITA' TECNICA

Ai sensi dell'art. 49 del D. Lgs 18.08.2000 n° 267, si esprime sulla proposta di deliberazione in oggetto parere *FAVOREVOLE* in ordine alla sola regolarità tecnica, dando atto che la presente proposta:

non comporta riflessi diretti o indiretti sulla situazione economico-finanziaria o sul patrimonio dell'ente;

Lì, 12/07/2019

IL DIRIGENTE
NICHELE EMANUELE
(Sottoscritto digitalmente ai sensi
dell'art. 21 D.L.gs n 82/2005 e s.m.i.)

COMUNE DI CITTADELLA

Cittadella Città d'Arte

PROVINCIA DI PADOVA

Proposta N. 2019 / 1379
SERVIZIO CED

OGGETTO: APPROVAZIONE DISCIPLINARE PER L'UTILIZZO DELLE RISORSE INFORMATICHE E TELEFONICHE DEL COMUNE DI CITTADELLA.

PARERE IN ORDINE ALLA REGOLARITA' CONTABILE

Parere del Responsabile di Ragioneria in ordine alla regolarità contabile (art. 49, comma 1, D. Lgs 18.08.2000 n. 267, così come sostituito dall'art. 3 del D.L. 174/2012) :

parere *FAVOREVOLE*

Lì, 12/07/2019

IL DIRIGENTE
SARTORE CARLO
(Sottoscritto digitalmente ai sensi dell'art. 21 D.L.gs n 82/2005 e s.m.i.)