Città di **Vicenza**

Insignita di due Medaglie d'Oro al Valore Militare
per il Risorgimento e la Resistenza

DISCIPLINARE SULL'UTILIZZO DEGLI STRUMENTI INFORMATICI E DELLA POSTA ELETTRONICA

approvato con D.G.C. nr 16 del 12/02/2025

Versione	**Attività**	**Data**
Rev.01	Produzione	12/02/2025
	Revisione	

GLOSSARIO

Nel presente Disciplinare sono state adottate le seguenti definizioni.

Ente: il Comune di Vicenza.

Titolare del trattamento: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali.

Responsabile del trattamento: la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che tratta dati personali per conto del titolare del trattamento ai sensi dell'art. 28 Regolamento UE 679/16.

Trattamento: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione.

Dati personali: qualunque informazione relativa a persona fisica, identificata o identificabile, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione o un identificativo on line.

Risorse ICT: gli apparati e dispositivi (es. PC, notebook, smartphone, tablet, ecc.), gli apparati di telecomunicazione, i sistemi informativi, sia hardware che software dell'Ente.

Amministratore di sistema: la figura professionale finalizzata alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti, ivi compresi gli amministratori di basi di dati, gli amministratori di reti e di apparati di sicurezza e gli amministratori di sistemi software complessi.

Violazione di dati personali: la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.

SIC: Settore Informatico Comunale dell'Ente.

1. PREMESSE

1.1. Scopo del Disciplinare

Il presente disciplinare (di seguito il "Disciplinare") determina le regole per il corretto ed adeguato accesso ed utilizzo di tutte le Risorse ICT dell'Ente, nonché del patrimonio informativo del Comune di Vicenza, quale Titolare del trattamento, al fine di:

- informare i soggetti che trattano dati con le risorse informatiche di quali sono le misure di tipo organizzativo e tecnologico adottate all'interno dell'Ente per la sicurezza dei dati;
- illustrare quali sono le modalità di utilizzo consapevole e diligente delle risorse messe a disposizione;
- ridurre i rischi relativi alle minacce di sicurezza informatica, preservando la disponibilità, integrità e confidenzialità dei dati e la continuità dei servizi erogati;
- evitare comportamenti inconsapevoli che possano innescare problemi o minacce alla sicurezza nel trattamento dei dati;
- comunicare agli utenti le finalità e le modalità dei controlli che l'Ente potrebbe effettuare sulle risorse messe a disposizione;
- fornire agli utenti una serie di indicazioni operative sulle corrette modalità di trattamento dei dati personali, delle informazioni e degli strumenti che permettono di gestirli, ad integrazione delle istruzioni già impartite.

1.2. Destinatari

Il Disciplinare si applica a:

- Amministratori e dipendenti dell'Ente, a qualsiasi titolo inseriti nell'organizzazione dell'Ente, senza distinzione di ruolo e/o livello;
- consulenti e collaboratori dell'Ente, a prescindere dal rapporto contrattuale intrattenuto con lo stesso;
- dipendenti e collaboratori di società che hanno un contratto in essere con l'Ente e che utilizzano Risorse ICT dello stesso;
- tutti i soggetti diversi dai precedenti a cui l'Ente consenta espressamente di utilizzare le Risorse ICT di proprietà dell'Ente stesso.

di seguito gli "Utenti".

1.3. Informativa sul trattamento dei dati personali e rispetto della Legge n. 300/1970

Gli strumenti tecnologici considerati nel presente Disciplinare costituiscono tutti strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa, anche ai sensi e per gli effetti dell'art. 4, comma secondo, della Legge n. 300/1970.

Il presente Disciplinare, nella parte in cui prevede le regole sull'utilizzo delle Risorse ICT e le tipologie di trattamenti di dati personali che possono essere svolti dall'Ente nell'ambito e in correlazione all'esecuzione dei controlli ai sensi dell'art. 4, comma 3, della Legge n. 300/1970, costituisce informativa ai sensi dell'art. 13 del Regolamento UE 679/2016, unitamente all'informativa allegata (Allegato 1).

I dati personali e le altre informazioni dell'Utente, che sono registrati nelle Risorse ICT e che si possono eventualmente raccogliere tramite il loro uso, sono utilizzati per finalità aziendali istituzionali, per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio dell'Ente, compresa la sicurezza informatica e la tutela del sistema informatico aziendale e sono utilizzabili per tutti i fini connessi al rapporto di lavoro, considerato che il presente Disciplinare costituisce adeguata informativa delle modalità d'uso degli strumenti e di effettuazione dei controlli da parte del datore di lavoro, fermo restando il rispetto della normativa in materia di protezione dei dati personali (Reg. UE 679/16 e D.lgs. n.196/2003).

1.4. Fonti normative

Il presente Disciplinare è stato redatto sulla base del Regolamento UE 679/16 ("Regolamento generale sulla protezione dei dati" o "GDPR"), del d.lgs. n. 196/2003 ("Codice privacy"), della L. n. 300/1970 ("Statuto dei Lavoratori") e delle "Linee Guida del Garante per posta elettronica e internet" pubblicate nella Gazzetta Ufficiale n. 58 del 10.03.2007, nonché degli altri provvedimenti in materia pronunciati dal Garante per la protezione dei dati personali (di seguito "il Garante"), dal Gruppo di lavoro Articolo 29 e dal Comitato Europeo per la Protezione dei dati, nonché del D.P.R. 16.04.2013 n. 62 "Regolamento recante codice di comportamento dei dipendenti pubblici, a norma dell'art. 54 del decreto legislativo 30 marzo 2001 n. 165", così come aggiornato con D.P.R. 13 giugno 2023, nr 81 e del vigente "Codice di comportamento del Comune di Vicenza".

1.5. Principi generali

Il presente Disciplinare si fonda sui medesimi principi espressi nel GDPR, in particolare:

a) principio di necessità, secondo il quale i sistemi informativi ed i programmi informatici devono essere configurati riducendo al minimo l'utilizzazione dei dati personali e dei dati identificativi in relazione alle finalità perseguite (articoli 5 e 6 GDPR);

b) principio di correttezza, secondo cui le caratteristiche essenziali dei trattamenti devono essere rese note ai lavoratori, in modo da renderli adeguatamente consapevoli;

c) trasparenza, secondo cui devono essere trasparenti le modalità con cui sono raccolti e utilizzati i dati personali;

d) principio di pertinenza e non eccedenza, secondo cui i trattamenti devono essere effettuati per finalità determinate, esplicite e legittime, nella misura meno invasiva possibile.

2. GESTIONE INGRESSO E USCITA DEGLI UTENTI

2.1. Avvio rapporto di lavoro

Al momento della formalizzazione del rapporto di lavoro con un nuovo Utente il Dirigente responsabile ne dà notizia al SIC secondo le procedure in essere.

E' cura del responsabile di Settore richiedere l'assegnazione di strumenti e dispositivi ICT quali, a titolo di esempio: casella di posta elettronica ordinaria, deleghe alle caselle di ufficio, account di dominio; accessi a banche dati, abilitazioni a servizi e applicazioni, dispositivi di autenticazione e di firma, cellulare di servizio, etc..

2.2. Modifica o cessazione del rapporto di lavoro

In caso di:

- cambiamento delle mansioni dell'Utente e/o spostamento presso altra Area;
- assegnazione delle risorse ICT ad altro Utente;
- cessazione del rapporto di lavoro a qualsiasi titolo

l'Utente è tenuto a comunicare la collocazione all'interno dei sistemi dell'Ente delle informazioni e della documentazione inerente l'attività lavorativa di interesse dell'Ente al proprio Responsabile o ad altro soggetto autorizzato a trattare le predette informazioni.

In caso di modifica delle mansioni dell'Utente o spostamento in altro Settore, il Dirigente responsabile provvederà a chiedere al SIC l'attivazione delle abilitazioni correlate al nuovo ruolo (es. accessi a banche dati, servizi e applicazioni, ecc). Le credenziali di accesso al dominio e la casella di posta elettronica ordinaria rimangono invece invariate.

Su comunicazione del Dirigente, in caso di cambio di ufficio/settore di un Utente il SIC provvederà a disabilitarne gli accessi relativi alle risorse afferenti all'ufficio precedente.

In caso di cessazione del rapporto di lavoro il SIC provvederà alla immediata disattivazione di tutte le credenziali e permessi in uso all'Utente.

È cura dell'Utente, prima del termine del proprio servizio, assicurarsi che nei dispositivi in uso non siano memorizzati informazioni, documenti o altri contenuti di natura personale non attinenti all'attività lavorativa; eventuali dati di carattere privato ancora presenti al momento della riconsegna della postazione verranno trattati secondo i principi di pertinenza e non eccedenza previsti dalla normativa sulla protezione dei dati personali. Decorsi 10 giorni dalla cessazione o modifica del rapporto di lavoro, l'Ente provvederà alla formattazione delle aree di memorizzazione dei dispositivi, sia locali che di rete. Lo stesso principio viene applicato per le cartelle nominative presenti nei server di rete.

3. REGOLE DI COMPORTAMENTO GENERALI

3.1. Finalità lavorative nell'utilizzo delle Risorse ICT

L'utilizzo delle Risorse ICT è consentito agli Utenti per finalità connesse allo svolgimento della propria attività lavorativa o ad essa riconducibile, nel rispetto e nei limiti del presente Disciplinare.

Gli Utenti sono tenuti ad utilizzare le Risorse ICT con diligenza, correttezza e buona fede, astenendosi dal porre in essere comportamenti che configurino illeciti di qualunque genere o violazione di diritti. Le Risorse ICT assegnate agli Utenti sono di proprietà dell'Ente e costituiscono strumenti di lavoro. Gli Utenti sono responsabili dei propri dispositivi e devono custodirli con cura, evitando ogni possibile forma di danneggiamento e segnalando tempestivamente ogni

malfunzionamento. Ogni utilizzo non inerente all'attività lavorativa può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza.

Non è permesso caricare, memorizzare, pubblicare, diffondere, distribuire, copiare tramite risorse dell'Ente documenti, informazioni, immagini, filmati etc. che siano:

- di carattere violento, pornografico o contrario alla pubblica decenza, o suscettibile di mancare di rispetto agli esseri umani o alla loro dignità, con contenuto discriminatorio razziale ed etnico, contrario al buon costume, oltraggioso, contrario all'ordine pubblico, diffamatorio o che contenga contenuti illeciti penalmente o civilmente riconducibili a categorie qui non espressamente indicate;
- illeciti in base alla normativa sul diritto d'autore;
- pregiudizievoli per le risorse dell'Ente, per la sua immagine, per l'integrità e la conservazione dei dati dell'Ente stesso.

Non è consentito permettere l'utilizzo da parte di soggetti non abilitati delle risorse dell'Ente, né consentire l'accesso ai dati e ad alle informazioni riservate, se non nei casi espressamente previsti dalla legge e/o da regolamenti interni.

Fermo restando quanto sopra, ai dipendenti è consentito l'utilizzo delle Risorse ICT per poter assolvere alle incombenze personali senza doversi allontanare dalla sede di servizio, purchè l'attività sia contenuta in tempi ristretti e senza alcun pregiudizio per i compiti istituzionali e a condizione che l'Utente:

- si attenga esclusivamente alle prescrizioni indicate nel presente Disciplinare, per cui sono definiti specifici limiti definiti per ogni tipologia di risorsa;
- sia esplicito verso terzi che la responsabilità di qualsiasi operazione svolta per finalità personali sia imputabile esclusivamente all'Utente;
- non sia contrario alle regole di condotta indicate nei paragrafi successivi e non possa in alcun modo ledere l'immagine dell'Ente;
- non danneggi in alcun modo, diretto o indiretto, le proprietà dell'Ente;
- non comporti alcuna violazione di leggi;
- non comprometta le misure di sicurezza e di protezione dei dati attuate e definite dalle politiche di sicurezza dell'Ente.

E' importante precisare che è consentito l'utilizzo privato esclusivamente delle risorse strumentali, ma non delle informazioni trattate per conto dell'Ente; non è in alcun modo consentito trattare dati di cui l'Ente è titolare del trattamento se non per attività strumentali al perseguimento delle finalità istituzionali dell''Ente.

3.2. Obbligo di riservatezza

Gli Utenti sono tenuti a non rivelare a terzi le caratteristiche delle Risorse ICT, le modalità di funzionamento e le norme di sicurezza adottate.

Gli obblighi di riservatezza previsti nel presente articolo sono vigenti e vincolanti anche dopo la cessazione del rapporto lavorativo.

3.3. Impostazioni

Le risorse ICT vengono consegnate agli Utenti con una configurazione coerente con le misure organizzative e di sicurezza impostate dall'Ente. L'esecuzione automatica dei contenuti dinamici (es. macro) presenti nei file deve essere mantenuta disattivata.

E' vietato, salvo autorizzazione del SIC, modificare le impostazioni delle risorse ICT a disposizione.

4. REGOLE DI COMPORTAMENTO SPECIALI RELATIVE ALL'UTILIZZO DEI PERSONAL COMPUTER E ALTRI DISPOSITIVI

4.1. Credenziali di autenticazione

L'accesso agli strumenti dell'Ente è protetto da password. Per l'accesso devono essere utilizzati almeno username e password.

4.2. Installazione e utilizzo di programmi

Non è consentito all'Utente di modificare le caratteristiche impostate sul proprio PC, salvo autorizzazione esplicita del SIC.

Non è consentito disinstallare o installare autonomamente programmi provenienti dall'esterno salvo previa autorizzazione del SIC, il quale, in rispondenza alle politiche di sicurezza dell'Ente ed alla normativa vigente, verificherà l'opportunità (in termini di sicurezza dei sistemi) dell'installazione, onde evitare il grave pericolo di introdurre vulnerabilità, virus, nonché di alterare la stabilità delle applicazioni del PC.

L'acquisto e la conseguente installazione di software devono essere sempre preventivamente valutati, autorizzati ed effettuati in collaborazione con il SIC, al fine di garantire la stabilità dei sistemi presenti e la compatibilità del software con gli stessi, nel rispetto delle procedure di procurement in vigore.

Non è consentito l'uso di programmi diversi da quelli messi a disposizione o autorizzati dall'Ente, in quanto l'inosservanza di questa disposizione, oltre al rischio di danneggiamenti del sistema per incompatibilità con il software esistente, può esporre l'Ente a gravi responsabilità civili e penali in caso di violazione della normativa sulla tutela del diritto d'autore (Legge 633 del 22 aprile 1941 sulla tutela della proprietà intellettuale), che impone la presenza nel sistema di software provvisto di regolare licenza d'uso.

È obbligatorio consentire l'installazione degli aggiornamenti di sistema che vengono proposti automaticamente, al primo momento disponibile, in modo da mantenere il PC sempre protetto.

Gli Utenti che sono in possesso di privilegi amministrativi attraverso i quali hanno la possibilità di effettuare installazioni sulla postazione di lavoro devono comunque richiedere l'autorizzazione al SIC prima di procedere all'installazione. Esclusivamente in casi eccezionali di motivata urgenza gli Utenti possono procedere all'installazione, formalizzando l'autorizzazione successivamente. In questo caso le verifiche di sicurezza (virus, vulnerabilità, compatibilità con il sistema, etc…) che

normalmente vengono effettuate dal SIC prima dell'inserimento di un software del sistema informatico, dovranno essere condotte da chi effettua l'installazione.

È vietato disattivare e/o disinstallare e/o modificare nella loro impostazione iniziale i sistemi antivirus salvo esplicita autorizzazione da parte del SIC.

4.3. Supporti esterni

L'utilizzo di supporti portatili infetti (chiavette USB, CD, Hard Disk..) è tra le cause principali di diffusione dei virus informatici; è pertanto consentito l'utilizzo di supporti portatili esclusivamente se forniti dall'Ente.

4.4. Violazioni di sicurezza, smarrimento o furto delle Risorse ICT

Nel caso in cui l'Utente venga a conoscenza di una qualsiasi violazione di sicurezza che possa comportare la violazione di dati personali, dovrà applicare le procedure previste dall'Ente per la gestione del data breach. In caso di smarrimento o furto di Risorse ICT, l'Utente dovrà sporgere regolare denuncia presso l'Autorità Giudiziaria.

4.5. Spegnimento del PC e allontanamento dalla propria posizione

Il PC deve essere spento dall'Utente che ne ha effettuato l'accesso al termine di ogni giornata lavorativa, al momento di lasciare gli uffici a fine giornata o prima, in caso di uscita anticipata dal luogo di lavoro.

Durante la giornata lavorativa, nelle pause, o, comunque, nei momenti in cui il PC rimanga anche solo temporaneamente incustodito per allontanamento dalla postazione di lavoro, l'Utente è tenuto scollegarsi dal sistema o bloccare l'accesso (**Tasti Windows+L**). 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.

4.6. Salvataggio dei documenti all'interno della rete informatica

Le unità di rete sono soggette a regolari attività di controllo, messa in sicurezza, amministrazione e back up da parte del SIC al fine di garantire la disponibilità e riservatezza dei dati in esse memorizzati.

La gestione dei dati e dei documenti su PC è demandata all'Utente che dovrà provvedere di norma alla loro memorizzazione nelle cartelle di rete condivise.

Dati ed informazioni archiviati dall'utente nella memoria locale del PC (incluso il desktop) non sono oggetto delle attività di messa in sicurezza sopra descritte: l'utente è pertanto responsabile di una loro eventuale perdita o compromissione.

Costituisce buona prassi effettuare con cadenza periodica (almeno ogni sei mesi) la pulizia degli archivi presenti sulla propria postazione e nelle cartelle di rete di propria competenza, con cancellazione dei file inutili o obsoleti. Si deve porre particolare attenzione ad evitare un'archiviazione ridondante con duplicazione dei dati.

E' ammessa la custodia di dati privati negli strumenti forniti in dotazione a condizione che:

- siano riposti in cartelle di cui sia esplicitamente indicata la privatezza del dato (es. cartelle con dicitura “personale”);

- siano esplicitamente differenziabili dai dati trattati per attività strumentali al perseguimento delle finalità istituzionali;

- vengano rimossi prima della riconsegna delle risorse fornite;

- non siano in alcun modo riposti su sistemi server e/o altre risorse di archiviazione fruibili attraverso condivisioni di rete.

4.7. Assenze

In caso di assenza dell'Utente, al fine di garantire la sicurezza e la continuità delle attività istituzionali, e qualora sussistano necessità d'ufficio, il Responsabile di Settore potrà richiedere agli Amministratori di Sistema di accedere con password amministrativa alle informazioni necessarie per il proseguimento dell'attività, ai sensi dell’art. 13 del presente Disciplinare. L'intervento sarà comunicato all'Utente e verrà redatto un apposito verbale nel quale riportare le necessità che abbiano determinato l’intervento. Dopo l’accesso, l’Utente dovrà provvedere al cambio password.

4.8. Antivirus

Il sistema informatico dell’Ente è protetto da software antivirus aggiornato quotidianamente.

L'attività di installazione, attivazione e manutenzione dei firewall, dei programmi antimalware e di sicurezza della navigazione è riservata al SIC. E' vietato quindi disattivare e/o disinstallare e/o modificare nella loro impostazione iniziale i firewall, i programmi antimalware e di sicurezza della navigazione installata sia a livello di server che di ogni singolo client, in quanto pericoloso per il proprio computer e per l'intera rete dell’Ente.

Nel caso il software antivirus rilevi la presenza di un virus l’Utente dovrà immediatamente spegnere il computer e segnalare l’accaduto al SIC.

Ogni Utente deve tenere comportamenti tali da ridurre il rischio di attacchi al sistema informatico aziendale mediante virus, **deve astenersi dall'aprire allegati ai messaggi di posta elettronica quando provengano da indirizzo o mittenti sconosciuti, nonché astenersi dal navigare su siti internet che appaiono non sicuri**. **I messaggi di posta elettronica di cui non si è certi della provenienza non devono mai essere aperti,** in quanto tali messaggi possono far parte di attività di “phishing” (messaggi che simulano, nella grafica e nel contenuto, quello di una istituzione nota al destinatario ma provengono in realtà da soggetti il cui scopo è il furto di identità). Tali messaggi devono immediatamente essere segnalati al SIC.

4.9. Utilizzo di notebook e altri dispositivi mobile

Le disposizioni del presente Disciplinare si applicano anche ai notebook e altri dispositivi con relativi software e applicativi, ove compatibili.

L’utente deve attivare sistemi di blocco schermo con protezione con password numerica o con segno grafico composto sullo schermo.

L'Utente assegnatario è responsabile della custodia del notebook e dovrà adottare le necessarie cautele al fine di evitare furti o indebiti utilizzi da parte di terzi, soprattutto in caso di trasferte.

In caso di smarrimento e/o furto, l'Utente assegnatario ha l'obbligo di informare per iscritto, entro 24 ore, anche via e-mail, il SIC al fine di approntare le necessarie misure di mitigazione del danno. L'Utente dovrà anche sporgere denuncia presso le sedi competenti, inoltrando poi copia della denuncia all'Ente.

4.10. Dismissione dei dispositivi

I dispositivi non funzionanti vanno immediatamente consegnati al SIC per lo smaltimento in sicurezza. La cancellazione dei dati avviene con modalità sicure tali da rendere irrecuperabile il dato ed impedirne la disponibilità ad alcun soggetto nel rispetto delle *best practice* in materia.

4.11. Gestione chiavi e dispositivi di autenticazione

Per lo svolgimento delle proprie attività professionali, gli Utenti possono essere dotati di chiavi o altri strumenti di autenticazione (es. smartcard, chiavi RFID, codici alfanumerici) per accedere alle risorse informatiche dell'Ente.

Gli Utenti sono tenuti ad utilizzare tali strumenti con la massima cautela, garantendone la messa in sicurezza. Tali strumenti non devono essere lasciati incustoditi in zone a libero accesso, al fine di ridurre il rischio di furti. In caso di trasferte, non devono essere lasciati in macchina, nemmeno per brevi periodi, in parcheggi pubblici o comunque zone non custodite.

Qualora tali strumenti dovessero essere smarriti o rubati, l'affidatario deve immediatamente segnalare l'evento al SIC, al fine di approntare le necessarie misure di mitigazione del danno.

4.12. Informazioni sulla conservazione dei dati

I log relativi all'utilizzo dei PC, reperibili nella memoria dei PC stessi ovvero sui server, nonché i file con essi trattati sono registrati e sono conservati per un tempo la cui durata è funzione della dimensione del file di log del dispositivo stesso e possono essere oggetto di controllo da parte del Titolare del trattamento, attraverso l'Amministratore di Sistema, per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale. I controlli possono avvenire secondo le disposizioni previste dall'articolo 13 del presente Disciplinare.

Le informazioni eventualmente raccolte sono altresì utilizzabili per tutti i fini connessi al rapporto di lavoro, compresa la verifica del rispetto del presente Disciplinare, considerato che il presente Disciplinare adeguata informazione sulle modalità d'uso degli strumenti e sulla effettuazione dei controlli ai sensi del GDPR.

5. REGOLE DI COMPORTAMENTO SPECIALI RELATIVE ALL'USO DELLA RETE DELL'ENTE

5.1. Accesso alla rete informatica

Per l'accesso alla rete informatica ciascun Utente deve essere in possesso delle specifiche credenziali di autenticazione. Le password d'ingresso alla rete e ai programmi sono segrete e vanno comunicate e gestite secondo le procedure impartite. **E' assolutamente proibito entrare nella rete e nei programmi con altri nomi Utente.**

E’ vietato connettere alla rete dell’Ente apparati volti a effettuare connessioni con reti esterne (es. router, switch, access point wireless, ecc.). E’ vietato anche il collegamento di pc personali alla rete comunale da parte degli utenti.

In caso sia necessario consentire ad un Utente l’accesso remoto alle risorse informative, questo deve essere preventivamente concordato con il SIC.

5.2. Cartelle di rete

Le cartelle di rete sono aree di condivisione di informazioni strettamente lavorative e non possono in alcun modo essere utilizzate per scopi diversi. **Tutte le informazioni rilevanti per l’attività lavorativa devono essere salvate nelle cartelle di rete presenti nei server dell’Ente.** Qualunque file che non sia legato all’attività lavorativa non può essere dislocato, nemmeno per brevi periodi, in queste unità, che hanno finalità esclusivamente lavorativa (es. documenti, fotografie, video, musica, pratiche personali, e-mail, film e quant’altro).

Sulle unità di rete vengono svolte regolari attività di controllo, amministrazione e back up da parte del SIC. **Tutte le unità diverse da quelle comuni non sono oggetto di back up**.

Di conseguenza le stesse non devono ospitare dati di interesse dell’Ente poiché non sono garantite la sicurezza e la protezione contro la loro eventuale perdita. Si specifica che la cartella “desktop” si trova sulla postazione in locale, pertanto è inadatta al salvataggio dei file in quanto non sottoposta a procedure di backup.

Gli Amministratori di Sistema, a seguito di interventi di sicurezza informatica e/o di manutenzione/aggiornamento, possono in qualunque momento procedere alla rimozione di ogni file o applicazione che riterrà essere pericolosi per la sicurezza sia sui PC degli Utenti sulle unità di rete, ferma restando ogni responsabilità civile, penale e disciplinare.

Per la trasmissione di file all’interno dell’organizzazione è possibile utilizzare la posta elettronica, prestando attenzione alla dimensione degli allegati, oppure è possibile utilizzare le cartelle di scambio create a tale scopo.

5.3. Piattaforme di file sharing

E’ possibile utilizzare piattaforme di file sharing solo se incluse tra le piattaforme consentite dal SIC o facenti parte della dotazione dell’Ente.

È vietato salvare documenti dell’Ente su supporti rimovibili o su piattaforme commerciali non autorizzate (es. Dropbox, GoogleDrive, OneDrive etc..).

5.4. Informazioni sulla conservazione dei dati

I log relativi all’uso della rete dell’Ente nonché i file salvati o trattati su server sono registrati e conservati per un tempo la cui durata è funzione della dimensione del file di log del dispositivo stesso e possono essere oggetto di controllo da parte del Titolare, attraverso l’Amministratore di Sistema, per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale. I controlli possono avvenire secondo le disposizioni previste dall’articolo 13 del presente Disciplinare.

Le informazioni eventualmente raccolte sono altresì utilizzabili per tutti i fini connessi al rapporto di lavoro, compresa la verifica del rispetto del presente Disciplinare, considerato che il presente Disciplinare costituisce adeguata informazione sulle modalità d'uso degli strumenti e sulla effettuazione dei controlli ai sensi del GDPR.

6. CREDENZIALI DI AUTENTICAZIONE

6.1. Composizione della password

La password deve rispettare le policy di sicurezza stabilite dal SIC e non contenere riferimenti agevolmente riconducibili all'Utente (username, nomi o date relative alla persona o a un suo familiare). La password non deve coincidere con altre password utilizzate dall'Utente per finalità personali (ad esempio password per l'accesso ai propri profili sociale, ecc.).

La password deve essere modificata dall'Utente al primo utilizzo e successivamente, almeno ogni 3 (tre) mesi o comunque secondo le regole di sicurezza implementate dall'Ente. La nuova password deve essere diversa da quella precedente.

Nel caso di inserimento di password errata, dopo un numero di tentativi dipendenti dal contesto informatico di utilizzo, il profilo dell'Utente potrebbe venire disabilitato e in questo caso sarà possibile richiederne la riattivazione agli Amministratori di Sistema.

Qualora l'Utente utilizzi credenziali amministrative di un sistema o ambiente (applicativo o sistemistico) che tratti dati di altri soggetti, la password deve essere di almeno 14 caratteri e deve attenersi alla disposizioni di AgId in materia di autenticazione.

6.2. Divieti e regole di comportamento

La password deve essere custodita dall'Utente con la massima diligenza e non deve essere divulgata nel modo più assoluto: cedere le proprie credenziali, ovvero permettere a terzi l'accesso ai servizi comunali, significa autorizzarli a proprio nome alla gestione degli stessi, con effetti potenzialmente gravissimi (ad es. visualizzazione di informazioni riservate, alterazione o distruzione di dati, uso della propria posta elettronica etc.).

È vietato quindi usare le credenziali di autenticazione di altro Utente nonché consentire ad altro Utente o a terzi di utilizzare le proprie credenziali di autenticazione.

E' vietato annotarsi la password su *post it* o altri biglietti collocati in prossimità del PC o in luoghi accessibili a terzi.

Nel caso in cui l'Utente sospetti che la password sia stata utilizzata da persone non autorizzate, dovrà darne immediata comunicazione al SIC. La password deve essere modificata dall'Utente qualora sospetti che la stessa non sia più segreta.

Qualora un Utente o qualsiasi altro soggetto dovesse venire a conoscenza della password di un altro Utente, è tenuto a darne immediata notizia all'interessato, astenendosi dal qualsiasi utilizzo o divulgazione degli stessi. L'interessato dovrà provvedere alla loro immediata modifica.

Gli Utenti devono proteggere le credenziali memorizzate sugli smartphone, tablet e p.c. utilizzati per fruire dei servizi dell'Ente (ad es. posta elettronica, intranet, ecc.) e, nel caso di furto o

smarrimento siano essi personali o dell'Ente, devono cambiare tempestivamente la "password del dominio".

6.3. Sospensione e disattivazione

Gli Amministratori di Sistema nominati dall'Ente per l'espletamento delle proprie funzioni nonché in caso di emergenza o di assenza dell'Utente, hanno la facoltà in qualunque momento di sospendere e/o modificare l'operatività dei profili personali degli Utenti (compresa la posta elettronica e la navigazione Internet) con le modalità e nei casi previsti dal presente Disciplinare.

7. UTILIZZO DI INTERNET

7.1. Finalità lavorative nell'uso di internet

La navigazione in internet è consentita esclusivamente per finalità collegate all'attività lavorativa, o alla stessa riconducibile, svolta dall'Utente, salvo la necessità di assolvere incombenze personali senza doversi allontanare dalla sede lavorativa, purchè l'attività sia contenuta in tempi ristretti e senza pregiudizio per i compiti istituzionali. Fermo restando quanto sopra, ciascun Utente deve attenersi alle seguenti regole di utilizzo della rete Internet e dei relativi servizi:

- l'accesso è consentito tramite firewall dell'Ente con le sue policy di sicurezza debitamente implementate e aggiornate;
- 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 e di qualunque tipo di software gratuito (freeware) o shareware prelevato da siti Internet, se non espressamente autorizzato dagli Amministratori di Sistema, l'uso di servizi di rete con finalità ludiche o, comunque, estranee all'attività lavorativa, navigare su siti pornografici o pedopornografici;
- non è consentito navigare su siti di social network di qualsiasi natura (in via esemplificativa e non esaustiva: Facebook, Twitter, Instagram, ecc...), salvo che per la gestione delle pagine istituzionali, utilizzare chat line (ad esclusione delle chat autorizzate per esigenze lavorative), iscriversi a forum non professionali.

L'Ente si riserva di bloccare l'accesso a siti considerati 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 dell'Ente, contattare il SIC per uno sblocco selettivo.

Il SIC 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.

7.2. Partecipazioni a social network

L'utilizzo e la consultazione di social network a fini promozionali 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 o collaboratori.

Le modalità di utilizzo dei social media sono disciplinati dal vigente Codice di Comportamento del Comune di Vicenza a cui si rimanda integralmente.

7.3. Rete WIFI

All'interno dei locali dell'Ente è presente la rete Wi-Fi pubblica che il Comune di Vicenza ha istituito per consentire la navigazione in Internet ai propri visitatori. L'accesso è alla rete Wi-Fi è protetto da password che non può essere diffusa senza esplicita autorizzazione del SIC.

7.4. Informazioni sulla conservazione dei dati

L'Ente, tramite i propri Amministratori di Sistema, non effettua la memorizzazione sistematica delle pagine web visualizzate dal singolo Utente.

A fini statistici, di qualità del servizio e di sicurezza, l'occupazione di banda generata dal traffico internet e dallo scambio di posta elettronica è soggetta a periodiche verifiche e controlli da parte dell'Ente sotto forma di dati aggregati ed anonimi, in osservanza dei limiti posti dalla legge in materia di protezione dei dati personali.

Qualora i sistemi di sicurezza segnalino delle potenziali criticità che possano minare l'integrità dei dati e la stabilità del sistema stesso, potrebbero essere effettuati dei controlli sulla navigazione internet effettuata tramite la rete dell'Ente. Tali controlli si opereranno secondo stadi successivi:

- controlli generici sulle pagine visitate, senza che vengano tracciati gli Utenti che le visitano;
- controlli aggregati sulle pagine visitate con suddivisione del traffico effettuato per aree lavorative;
- controlli specifici sulle pagine visitate, con tracciamento dell'indirizzo IP da cui si effettua la visita o dell'Utente che la effettua.

I controlli aggregati e specifici verranno effettuati solo qualora i trattamenti generici non abbiano consentito di risolvere le criticità riscontrate e verranno comunque segnalati in forma preventiva agli Utenti, in conformità all'art. 13 del presente Disciplinare.

Il sistema di registrazione dei log è configurato per cancellare periodicamente ed automaticamente (attraverso procedure di sovrascrittura) i dati personali degli Utenti relativi agli accessi internet ed al traffico telematico la cui conservazione non sia necessaria.

I file di log vengono conservati per il periodo strettamente necessario per il perseguimento delle finalità organizzative, produttive e di sicurezza, e comunque non oltre 30 giorni, fatti salvi in ogni caso specifici obblighi di legge.

L'eventuale prolungamento dei tempi di conservazione sarà valutato come eccezionale e potrà avere luogo solo in relazione a:

- esigenze tecniche o di sicurezza del tutto particolari;

- indispensabilità del dato rispetto all'esercizio o alla difesa di un diritto in sede giudiziaria;
- obbligo di custodire o consegnare i dati per ottemperare ad una specifica richiesta dell'autorità giudiziaria o della polizia giudiziaria.

I file di log sono accessibili solo agli Amministratori di Sistema.

Le informazioni eventualmente raccolte sono altresì utilizzabili per tutti i fini connessi al rapporto di lavoro, compresa la verifica del rispetto del presente Disciplinare, considerato che il presente Disciplinare costituisce adeguata informazione sulle modalità d'uso degli strumenti e sulla effettuazione dei controlli ai sensi del GDPR.

8. UTILIZZO DELLA POSTA ELETTRONICA

8.1. Finalità lavorative nell'utilizzo della posta elettronica

La posta elettronica messa a disposizione dall'Ente è uno strumento di lavoro: è fatto divieto di utilizzare qualunque account di posta istituzionale per finalità diverse da quelle connesse all'attività lavorativa o ad essa riconducibili e nel caso in cui l'utilizzo possa compromettere la sicurezza o la reputazione dell'Ente. L'Utente è responsabile del corretto utilizzo della casella di posta elettronica e del contenuto dei messaggi inviati.

Gli indirizzi di posta elettronica individuali sono così predisposti mrossi@comune.vicenza.it. L'Ente 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 singoli Utenti mantengano l'esclusività su dati dell'Ente.

Non è consentito l'inoltro o il re-indirizzamento di e-mail aziendali all'indirizzo e-mail privato, anche durante i periodi di assenza (es. ferie, malattia, ecc.); tale comportamento pone a rischio il patrimonio informativo aziendale e costituisce violazione della normativa sulla protezione dei dati.

Non è consentito l'utilizzo di caselle di posta elettronica personali diverse da quelle istituzionali per le comunicazioni istituzionali salvo casi di forza maggiore dovuti a circostanze in cui il dipendente, per qualsiasi ragione, non possa accedere all'account istituzionale.

È fatto divieto di inviare/partecipare a catene telematiche via e-mail. In caso di ricezione di e-mail non attinenti alle attività di lavoro (spam), queste vanno immediatamente eliminate, senza aprire gli allegati di tali messaggi.

L'iscrizione a mailing-list o newsletter esterne, con il proprio indirizzo personale istituzionale è concessa esclusivamente per motivi professionali. Prima di iscriversi occorre verificare l'affidabilità del sito che offre il servizio.

E' fondamentale rilevare che l'utilizzo della casella di posta elettronica è strumentale all'attività istituzionale dell'Ente, ma non è il canale ufficiale per le comunicazioni che impegnino l'Ente verso terzi. Per tutti quei procedimenti aventi rilevanza esterna, le comunicazioni dovranno essere veicolate attraverso canali collegati al protocollo informatico dell'Ente, come la posta elettronica certificata istituzionale.

8.2. Regole di comportamento

Gli Utenti sono tenuti a rispettare le seguenti regole di condotta:

- è obbligatorio uniformarsi alle modalità di firma dei messaggi di posta elettronica individuate dall'Ente, comunicato al momento dell'assegnazione della casella di posta.
- ciascun messaggio di posta elettronica deve consentire l'identificazione del dipendente mittente e deve indicare un recapito istituzionale al quale il medesimo è reperibile;
- è obbligatorio porre la massima attenzione nell'aprire i file attachments di posta elettronica prima del loro utilizzo (non scaricare file eseguibili o documenti di ogni genere da siti Web o Ftp non conosciuti);
- nel caso vi fosse incertezza in ordine alla credibilità del messaggio e/o alla sua provenienza l'Utente dovrà contattare immediatamente l'Amministratore di Sistema per una valutazione del singolo caso;
- mantenere in ordine la casella di posta elettronica, cancellando documenti inutili e soprattutto allegati ingombranti. È necessario prestare attenzione ed evitare la duplicazione dei dati;
- procedere alla pulizia periodica della casella almeno ogni sei mesi;
- è vietato inviare posta elettronica in nome e per conto di un altro Utente, salvo sua espressa autorizzazione;
- prima di inviare un messaggio di posta elettronica, assicurarsi che i destinatari selezionati ed i file allegati siano corretti;
- prestare particolare attenzione nel selezionare il comando "rispondi a tutti" nella corrispondenza e-mail;
- nel caso di invio a destinatario errato, inviare al soggetto ricevente una comunicazione con la quale lo si informa dell'errato invio, chiedendo l'immediata cancellazione della mail e degli eventuali allegati, inibendo qualsiasi utilizzo delle informazioni/documenti erroneamente inviati nonché chiedendo l'invio di una mail di conferma dell'adozione delle predette prescrizioni. Qualora la e-mail contenga dati personali nel corpo del testo oppure negli allegati, l'Utente dovrà segnalare l'evento secondo la procedura sul data breach adottata dall'Ente per le necessarie valutazioni;
- in caso di invio massivo di e-mail, i destinatari devono essere messi in copia nascosta (Bcc o Ccn), se la natura del messaggio lo permette;
- se l'e-mail ricevuta è destinata ad altre persone è necessario limitare il più possibile la lettura del documento, ovvero facendolo con il solo obiettivo di comprendere che non si tratta di documentazione propria ma inviare un messaggio al mittente spiegando l'errore. L'e-mail ricevuta va immediatamente eliminata, anche dal cestino;
- nel caso in cui fosse necessario inviare a destinatari esterni messaggi contenenti allegati con dati personali particolari o soggetti a particolare riservatezza, è obbligatorio che questi allegati vengano preventivamente resi inintelligibili attraverso crittografia con apposito software (archiviazione e compressione con password). La password di cifratura deve

essere comunicata al destinatario attraverso un canale diverso dalla e-mail (ad esempio per telefono) e mai assieme ai dati criptati. Tutte le informazioni dell'Ente, i dati personali e/o particolari di competenza dell'Ente possono essere inviati soltanto a destinatari - persone o Enti – qualificati e autorizzati alla ricezione;

- è vietato l'invio di messaggi di posta elettronica, all'interno o all'esterno dell'amministrazione, che siano oltraggiosi, discriminatori o che possano essere in qualunque modo fonte di responsabilità dell'amministrazione.

Al fine di garantire la continuità dell'attività istituzionale nonché di provvedere alla dovuta conservazione della documentazione in base alla normativa applicabile, gli Utenti devono provvedere all'archiviazione nelle preposte cartelle di rete di tutti i documenti rilevanti ai fini lavorativi inclusi in particolare gli allegati alle e-mail.

8.3. Assenza dell'Utente

Per gli indirizzi e-mail nominativi, al fine di garantire la funzionalità del servizio di posta elettronica e di ridurre al minimo l'accesso ai dati, nel rispetto del principio di necessità e di proporzionalità, in caso di assenze programmate (ad es. per ferie), l'Utente dovrà impostare la risposta automatica di assenza dall'ufficio contenente le indicazioni alternative per contattare l'ufficio.

In caso di assenza non programmata (ad es. per malattia) la procedura - qualora non possa essere attivata dal lavoratore avvalendosi del servizio webmail entro due giorni - verrà attivata a cura dell'Amministratore di Sistema, su richiesta scritta del Responsabile di Settore. Nel caso in cui l'Utente sia Responsabile di Settore, la richiesta può essere effettuata dal direttore medesimo, ovvero dal Direttore Generale.

Qualora non fosse possibile attivare la funzione sopra descritta e/o 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 Responsabile di Settore quelli ritenuti rilevanti per lo svolgimento dell'attività lavorativa. L'accesso alla casella dell'utente assente può venire per motivate esigenze di ufficio anche su istanza del Responsabile di Settore. Sarà compito del Responsabile di Settore assicurarsi che sia redatto un verbale attestante quanto avvenuto e che sia informato il lavoratore interessato alla prima occasione utile. Nel caso in cui l'Utente sia Responsabile di Settore, la richiesta può essere effettuata dal direttore medesimo, ovvero dal Direttore Generale.

8.4. Disattivazione della casella di posta elettronica

La casella di posta elettronica, unitamente alle credenziali di autenticazione per l'accesso alla rete, viene disattivata entro **5 (cinque) giorni lavorativi** dalla comunicazione al SIC della conclusione del rapporto di lavoro che ne giustificava l'assegnazione da parte del Responsabile di Settore o delle Risorse Umane.

L'Utente è tenuto a trasmettere dati e informazioni di interesse istituzionale al proprio Responsabile o ad altro soggetto autorizzato a trattare i predetti dati, fermo restando quanto previsto nell'ultimo paragrafo dell'art. 8.2.

8.5. Informazioni sulla conservazione dei dati

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

I log relativi all'infrastruttura del sistema di posta verranno conservati per la durata di 21 gg per finalità organizzative, produttive e di sicurezza.

Per finalità organizzative di sicurezza e business continuity viene effettuato il back up della posta elettronica relativa agli **ultimi 30 giorni di attività.**

In seguito alla cessazione dell'Utente, la casella di posta viene eliminata definitivamente entro un mese. Il back up di posta elettronica viene conservato per 30 giorni dalla eliminazione della casella.

In caso di situazioni di contenzioso o di precontenzioso inoltre, le comunicazioni e-mail ed i documenti allegati potranno essere conservati per il tempo necessario alla tutela dei diritti dell'Ente. Per situazioni di precontenzioso si intendono tutte quelle fattispecie in cui, in presenza di comportamenti rilevati e/o atti formalmente assunti, è presumibile il sorgere di un contenzioso.

9. UTILIZZO DI APPARATI DI TELEFONIA, FOTOCOPIATRICI, SCANNER E STAMPANTI

9.1. Finalità lavorative nell'utilizzo degli apparati di telefonia e di stampa

Gli apparati di telefonia (fissa, mobile e tablet) e gli strumenti di stampa sono di proprietà o noleggiati dall'Ente , possono essere utilizzati solo per finalità collegate all'attività lavorativa svolta dall'Utente per l'Ente e devono essere custoditi con diligenza.

Con riferimento a tutti gli apparati telefonici, fermo restando quanto sopra già disposto circa il loro uso e custodia, la ricezione o l'effettuazione di telefonate personali, così come l'invio o la ricezione di messaggi di natura personale o comunque non pertinenti rispetto allo svolgimento dell'attività lavorativa, viene consentita solo nel caso di comprovata necessità ed urgenza.

Le disposizioni del presente paragrafo vanno applicate anche alle sole schede SIM e similari, per quanto compatibili.

Qualora venisse assegnato all'Utente un cellulare dell'Ente, l'Utente sarà responsabile del suo utilizzo e della sua custodia.

L'utilizzo di dispositivi mobili non deve minare la sicurezza dei dati e dei sistemi dell'Ente. Ai cellulari e smartphone dell'Ente si applicano le medesime regole sopra previste per gli altri dispositivi informatici, per quanto concerne il mantenimento di un adeguato livello di sicurezza informatica nonché le regole per la corretta navigazione in internet.

Non sono consentite manomissioni hardware o software sui dispositivi aziendali.

L'Utente deve attivare sistemi di blocco schermo con protezione con password numerica o con segno grafico composto sullo schermo. La password o PIN devono essere diverse da quelle utilizzate all'interno dell'Ente.

In caso di smartphone, è vietata l'installazione e l'utilizzo di Applicazioni ("App") non direttamente funzionali all'attività di servizio. In ogni caso si richiede massima cautela nell'installare nuove app perché potenziale fonte di vulnerabilità e minacce informatiche. In caso di dubbi rivolgersi al SIC.

Gli Utenti non devono utilizzare reti telematiche insicure per la trasmissione di dati (ad esempio, reti WiFi disponibili in locali pubblici, hotel, ecc.).

I dispositivi mobile di lavoro non devono essere utilizzati per motivi personali, pertanto non devono essere salvati, né nel dispositivo, né nella scheda di memoria rimovibile, dati, informazioni, foto di natura personale, salvo autorizzazioni specifiche.

Nel caso in cui sia autorizzato l'uso del dispositivo aziendale anche per uso personale, l'Utente è tenuto ad archiviare separatamente, ove compatibile con lo strumento assegnato, dati e informazioni inerenti all'attività lavorativa (es. foto, documenti) e ad adottare le opportune cautele per evitare che terzi non autorizzati possano prendere cognizione dei documenti e/o informazioni di pertinenza dell'Ente.

Al momento della restituzione del dispositivo all'Ente a seguito di cessazione del dipendente o per altra causa (es. assegnazione nuovo dispositivo), deve essere realizzata la cancellazione sicura delle informazioni per proteggere le informazioni riservate e i dati personali secondo la normativa vigente. L'Utente è tenuto **obbligatoriamente** ad eseguire la cancellazione dei dati, prima di restituire il dispositivo al SIC. L'Utente è tenuto a salvare su altri supporti eventuali dati o informazioni personali presenti sul dispositivo. L'ente non è responsabile di eventuali dati rimasti nel dispositivo.

In caso di furto o smarrimento dei dispositivi cellulari o della SIM assegnati l'Utente è tenuto a dare tempestiva comunicazione al SIC e a fare denuncia presso l'Autorità Giudiziaria al fine di consentire l'immediato blocco del dispositivo da remoto.

Gli strumenti di stampa possono essere utilizzati solo per finalità lavorative e devono essere custoditi con diligenza. È vietato l'utilizzo delle fotocopiatrici e di scanner per fini personali, salvo i casi di necessità e urgenza e comunque, non in modo ripetuto o per periodi di tempo prolungati.

Per quanto concerne l'uso delle stampanti gli Utenti sono tenuti a stampare documenti solo se strettamente necessari per lo svolgimento delle proprie funzioni operative. Prediligere le stampanti di rete condivise, rispetto a quelle locali/personali, per ridurre l'utilizzo di materiali di consumo (toner ed altri consumabili). In caso di stampanti condivise gli Utenti dovranno ritirare prontamente le stampe dai vassoi delle stampanti per evitare la possibile perdita o divulgazione di tali informazioni a persone terze non autorizzate.

10. GESTIONE RIUNIONI IN VIDEOCONFERENZA

L'Ente, tenuto conto dell'evoluzione delle nuove tecnologie, acconsente lo svolgimento di riunioni ed incontri, sia tra il personale interno che tra il personale e soggetti esterni, mediante videoconferenza. Tale modalità costituisce un'utile risorsa e una pratica soluzione volta a risolvere eventuali difficoltà logistiche, ottimizzando tempi e risorse.

In caso di riunioni aventi ad oggetto argomenti tecnici o comunque complessi o articolati, al solo fine di tenere traccia del contenuto dell'incontro, riducendo le difficoltà legate all'eventuale verbalizzazione, è possibile procedere alla registrazione degli incontri. È esclusa la registrazione per fini personali.

La registrazione è altresì esclusa qualora nel corso della riunione debbano essere trattate categorie di dati particolari ai sensi dell'art. 9 GDPR o dati giudiziari.

Considerato che la registrazione audio e video dei partecipanti costituisce un trattamento di dati personali, l'Ente è tenuto a rispettare le disposizioni della normativa sulla protezione dei dati personali.

La base giuridica del trattamento connesso alle videoconferenze ed eventuali registrazioni degli incontri è data dall'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri (art. 6. par. 1, lettera e) GDPR e art. 2 ter d.lgs. 196/2003).

In caso di riunione in videoconferenza, l'Utente deve attenersi alle seguenti istruzioni:

- inviare ai destinatari l'invito alla videoconferenza via e-mail, precisando che l'incontro si terrà in modalità remota;
- all'inizio della riunione, verificare l'effettiva identità dei partecipanti;
- assicurarsi che tutti i partecipanti possano intervenire in tempo reale all'incontro (è facoltà dei singoli partecipanti attivare o disattivare la telecamera, fermo restando la necessità di identificare previamente ~~i~~ gli stessi);
- qualora l'organizzatore della riunione ritenga di registrare l'incontro, lo stesso dovrà avvisare i partecipanti prima dell'inizio della riunione, informandoli della facoltà di disattivare le webcam, silenziare i microfoni e formulare quesiti/interventi via chat;
- qualora l'organizzatore della riunione ritenga di registrare l'incontro, lo stesso dovrà avvisare i partecipanti prima dell'inizio della riunione, informandoli della facoltà di disattivare le webcam, silenziare i microfoni e formulare quesiti/interventi via chat, precisando che la registrazione viene svolta per finalità di verbalizzazione nel rispetto della normativa sulla protezione dei dati e che l'informativa privacy è disponibile sul sito del Comune. Qualora uno dei partecipanti si opponga alla registrazione e la sua partecipazione alla riunione sia indispensabile, non si potrà procedere alla registrazione;
- qualora nella stanza da dove ci si collega siano presenti più persone, è necessario utilizzare idonei auricolari al posto dell'audio del PC o dell'altoparlante e adottare opportuni accorgimenti per evitare la ripresa di terzi;
- silenziare il proprio microfono quando non si deve intervenire.

Il presente articolo non si applica alle registrazioni delle sedute del Consiglio Comunale, soggette a diverso regolamento.

11. DISPOSITIVI BYOD (BRING YOUR OWN DEVICE)

Con il termine BYOD si fa riferimento alla possibilità di utilizzare un proprio dispositivo personale (smartphone, pc, etc..) per accedere alla rete e ai sistemi informatici dell'Ente.

L'utilizzo di dispositivi personali in ambito lavorativo, se da un lato garantisce maggiore flessibilità ed efficienza per il dipendente, dall'altro introduce rischi per la sicurezza derivanti dall'utilizzo promiscuo del dispositivo da parte dell'Utente, sia per finalità lavorative che private, con le conseguenti criticità correlate al trattamento dei dati.

E’ necessario quindi bilanciare il diritto alla protezione dei dati degli Utenti con le esigenze di sicurezza e gli obblighi che gravano sull’Ente quale titolare del trattamento dei dati, a prescindere dal fatto che i dati siano trattati tramite dispositivi non aziendali, tenendo conto dei seguenti fattori:

- Tipologia di dati trattati;
- luogo di conservazione dei dati;
- le modalità di trasferimento dei dati;
- la possibilità/probabilità di perdita di dati;
- la commistione tra dati privati e dati aziendali;
- il livello di sicurezza dei dispositivi;
- le procedure da seguire in caso di cessazione del rapporto di lavoro del dipendente;
- le procedure da seguire in caso di perdita, furto, malfunzionamenti del dispositivo.

Autorizzazione e Requisiti.
L’utilizzo di dispositivi personali da parte di un utente deve essere autorizzato per iscritto dal Responsabile di Settore. Se l’utente è Responsabile di Settore esso deve darne comunicazione al SIC.
L’Utente deve garantire che il dispositivo sia conforme ai requisiti tecnici e di sicurezza definiti dall’Ente. L’attivazione da parte del SIC delle procedure per l’accesso ai sistemi informatici dell’Ente da parte del dispositivo a è subordinata alla sottoscrizione di una dichiarazione di conformità di quest’ultimo da parte dell’Utente.

Sicurezza.
Tutti i dispositivi personali autorizzati devono avere un sistema operativo e applicazioni aggiornati, essere protetti da password sicure o autenticazione biometrica. Devono inoltre avere un software antivirus approvato e configurato secondo le direttive del SIC. L’accesso ai dati dell’Ente è consentito esclusivamente tramite VPN istituzionale o applicazioni ufficiali configurate dal SIC, come i client di posta elettronica autorizzati. È vietato salvare localmente sul dispositivo personale dati particolari o riservati; tutti i dati devono essere conservati nei server o nelle piattaforme ufficiali dell’Ente. Si ricorda che gli allegati ai messaggi di posta elettronica visualizzati dall’Utente vengono automaticamente salvati nella cartella “download”. Gli Utenti sono tenuti alla periodica eliminazione dalla predetta cartella dei documenti di rilevanza lavorativa.

Limitazioni d'uso.
I dispositivi personali possono essere utilizzati solo per attività lavorative specifiche, come l’accesso alla posta elettronica istituzionale o la partecipazione a videoconferenze. Non è consentito il trattamento di dati particolari o riservati al di fuori dai sistemi ufficiali. È vietato, nell’ambito della propria attività lavorativa, utilizzare piattaforme di cloud storage non autorizzate, connettersi a reti Wi-Fi pubbliche o insicure e installare software non approvati dall’Ente.

Gestione di Perdita, Furto o Malfunzionamento.
In caso di perdita, furto o malfunzionamento del dispositivo personale, l’Utente deve informare immediatamente il SIC fornendo i dettagli necessari. Il SIC può disabilitare l’accesso del dispositivo alle risorse dell’Ente e, se tecnicamente possibile, rimuovere i dati aziendali da remoto. L’Utente è tenuto a collaborare per attuare le misure di protezione dei dati richieste.

Responsabilità degli Utenti.

Gli Utenti sono responsabili del rispetto della politica e delle normative vigenti, in particolare quelle relative alla protezione dei dati personali. Devono segnalare tempestivamente al SIC eventuali violazioni, accessi non autorizzati o perdite di dati. Gli Utenti accettano inoltre che i dispositivi personali possano essere sottoposti a verifiche di conformità da parte del SIC, previo consenso.

Diritti e Limitazioni dell'Ente.
L'Ente si riserva il diritto di revocare l'autorizzazione all'utilizzo dei dispositivi personali in qualsiasi momento qualora emergano rischi per la sicurezza o violazioni della politica di sicurezza. L'Ente non è responsabile per danni, furti, smarrimenti o malfunzionamenti dei dispositivi personali utilizzati per scopi lavorativi.

Cessazione del Rapporto di Lavoro.
Alla conclusione del rapporto di lavoro l'Utente deve rimuovere tutti i dati e le applicazioni aziendali dal dispositivo, previa verifica del SIC. Se tecnicamente possibile, il SIC potrà eseguire un reset remoto delle configurazioni aziendali sul dispositivo.

12. ASSISTENZA AGLI UTENTI E MANUTENZIONI, ACCESSO AI DATI

Gli Amministratori di Sistema del SIC possono accedere ai dispositivi informatici dell'Ente sia direttamente, sia mediante software di accesso remoto, per i seguenti scopi:

- verifica e risoluzione di problemi sistemistici ed applicativi, su segnalazione dell'Utente;
- verifica del corretto funzionamento dei singoli dispositivi in caso di problemi rilevati nella rete, per la sicurezza e protezione del sistema informatico;
- provvedere a richieste di aggiornamento software e manutenzione preventiva hardware e software.

Gli interventi avvengono su richiesta dell'Utente e/o previo autorizzazione del medesimo, 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 alla sessione di lavoro dell'utente mediante credenziali utente, l'Amministratore di Sistema è autorizzato ad effettuare gli interventi senza il consenso dell'utente cui la risorsa è assegnata. Sono fatti salvi gli interventi urgenti necessari al fine di fronteggiare situazioni di emergenza, per i quali verrà comunque dato avviso agli Utenti interessati, salvo che ciò non pregiudichi la tempestività e/o efficacia dell'intervento. Nei predetti casi, l'Amministratore di Sistema potrà accedere ai dati trattati da ciascun Utente e procedere a tutte le operazioni di configurazione e gestione necessarie per garantire la corretta funzionalità del sistema informatico aziendale, inclusa la rimozione di file o applicazioni pericolose.

L'accesso in teleassistenza sui PC della rete dell'Ente richiesto da terzi (fornitori e/o altri) deve essere autorizzato dagli Amministratori di Sistema, per le verifiche delle modalità di intervento per il primo accesso. Le richieste successive, se effettuate con le medesime modalità, possono essere gestite autonomamente dall'Utente.

13. CONTROLLI

13.1. Principi generali

Le risorse messe a disposizione degli Utenti sono strumenti attraverso i quali vengono perseguiti gli obiettivi istituzionali, su cui l'Ente gode di diritti esclusivi di proprietà e utilizzo. Il Titolare ha diritto di ottenere una corretta prestazione lavorativa e di attuare misure di sicurezza idonee alla difesa del patrimonio informativo.

L'Ente, per mezzo del SIC, si riserva la facoltà di svolgere controlli difensivi e/o indiretti volti a verificare il rispetto delle prescrizioni del presente Disciplinare e di adottare ogni misura atta a garantire la sicurezza e la protezione dei sistemi informatici, delle informazioni e dei dati, nel rispetto della tutela del diritto alla riservatezza, del principio di proporzionalità, trasparenza, pertinenza, non eccedenza e minimizzazione dei dati. I controlli dovranno essere adeguati, pertinenti e non eccessivi rispetto alle finalità perseguite ed eseguiti in modo da evitare un'interferenza ingiustificata sui diritti e sulle libertà fondamentali dei lavoratori.

I controlli, ove possibile, verranno svolti preventivamente su informazioni appartenenti a gruppi collettivi di Utenti, su dati aggregati, per poi passare, in caso di persistenti anomalie, a controlli su base individuale, come di seguito descritto. Gli stessi saranno conformati a quanto stabilito mediante linee guida adottate dall'Agenzia per l'Italia Digitale, sentito il Garante per la protezione dei dati personali, quando disponibili.

In ogni caso sono esclusi controlli prolungati, costanti o indiscriminati o comunque preordinati al controllo a distanza dei lavoratori.

Si precisa che l'uso degli strumenti informatici dell'Ente può lasciare traccia delle informazioni sul relativo uso, come descritto nel presente Disciplinare. Tali informazioni, che possono contenere dati personali, anche particolari, riferibili all'Utente, possono essere oggetto di controlli da parte dell'Ente, tramite gli Amministratori di Sistema, volti a garantire esigenze organizzative e produttive, la sicurezza del lavoro e la tutela del patrimonio dell'Ente, la sicurezza e salvaguardia del sistema informatico e le ulteriori esigenze tecniche e/o manutentive. Gli interventi di controllo sono di due tipi, descritti nei punti 13.2 e 13.3, e possono permettere all'Ente di prendere indirettamente cognizione dell'attività svolta dagli Utenti.

13.2. Controlli per la tutela del patrimonio aziendale dell'ente, per la sicurezza e la salvaguardia del sistema informatico. Controlli per ulteriori motivi tecnici e/o manutentivi.

Qualora si renda necessario accedere agli strumenti informatici e Risorse ICT degli Utenti per motivi di sicurezza e protezione del sistema informatico (ad. es. contrasto ai virus, malware, intrusioni telematiche, ecc.), ovvero per motivi tecnici e/o manutentivi e/o di regolare svolgimento dell'attività lavorativa (ad es. aggiornamento/sostituzione ed implementazione di programmi, manutenzione hardware), presenza di utilizzi indebiti/abusi da parte degli Utenti, necessità di effettuare verifiche volte alla protezione del patrimonio dell'Ente, il Titolare del Trattamento, tramite il SIC, si atterrà alla procedura sotto descritta:

a) analisi aggregata del traffico di rete riferito all'intera struttura o a sue aree/settore è preceduto da un avviso generico a tutti i dipendenti o a quelli appartenenti all'Area/Settore interessati della presenza di comportamenti anomali che possono mettere a rischio la sicurezza del sistema informatico e richiamo all'esigenza di attenersi al rispetto del presente Disciplinare;

b) successivamente, almeno dopo 7 (sette) giorni, se il comportamento anomalo persiste, l'Ente potrà chiedere agli Amministratori di Sistema il controllo sulle Risorse ICT con possibilità di rilevare i file trattati, i siti web visitati, software installati, documenti scaricati, statistiche sull'uso di risorse, informazioni rilevate dai dispositivi di sicurezza (es. antivirus, firewall, ecc.) ecc., nel corso dell'attività lavorativa. Tale attività potrà essere effettuata in forma anonima ovvero tramite il controllo del numero IP dell'Utente e con l'identificazione del soggetto che non si attiene alle istruzioni impartite. Se in seguito all'avviso generalizzato le anomalie cessano, non si procederà a successivi controlli su base individuale;

c) 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 procedimentali descritti alle lettere a) e b), l'Ente, unitamente agli Amministratori di Sistema, può intervenire senza indugio sullo strumento da cui proviene la potenziale minaccia.

Qualora indirettamente si riscontrino file o informazioni, anche personali, essere potranno essere utilizzabili per tutti i fini connessi al rapporto di lavoro, considerato che il presente Disciplinare costituisce adeguata informazione sulle modalità d'uso degli strumenti e sulla effettuazione dei controlli ai sensi del GDPR.

13.3. Controlli per esigenze produttive e di organizzazione

Per esigenze produttive e di organizzazione si intendono, tra le altre, l'urgente ed improrogabile necessità di accedere a file o informazioni lavorative di cui si è ragionevolmente certi che siano disponibili su risorse informatiche di un Utente (quali file salvati, posta elettronica, 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 l'Ente, unitamente all'Amministratore di Sistema, si atterrà alla procedura qui di seguito descritta (se e in quanto compatibile con l'Apparato oggetto di controllo), limitandosi ad accedere ai documenti strettamente indispensabili.

a) redazione da parte del Responsabile di Settore o - nel caso in cui ill'utente sia Responsabile di Settore - del Direttore Generale, di un verbale che comprovi le necessità produttive e di organizzazione che richiedono l'accesso allo Strumento;

b) incarico all'Amministratore di Sistema di accedere alla risorsa con credenziali di Amministratore ovvero tramite l'azzeramento e contestuale creazione di nuove credenziali di autenticazione dell'Utente interessato, con avviso che al primo accesso alla risorsa, l'Utente dovrà provvedere alla sostituzione della password;

c) redazione di un verbale che riassuma le operazioni precedenti, sottoscritto dal Responsabile di Settore e dall'Amministratore di Sistema.

Qualora indirettamente si riscontrino file o informazioni, anche personali, essere potranno essere utilizzabili per tutti i fini connessi al rapporto di lavoro, considerato che il presente Regolamento costituisce adeguata informazione sulle modalità d'uso degli strumenti e sulla effettuazione dei controlli ai sensi del GDPR.

14. ENTRATA IN VIGORE E SANZIONI

Il presente Disciplinare entra in vigore nella data della sua approvazione e abroga tutte le disposizioni precedenti in materia, in qualsiasi forma comunicate.

Gli uffici competenti provvederanno a comunicare agli Utenti l'esistenza del presente disciplinare, la cui versione più recente potrà in ogni momento essere reperita presso la intranet dell'Ente e sarà comunque adeguatamente pubblicizzata mediante affissione in luogo accessibile ai sensi dell'art. 7 Legge 300/1970.

È fatto obbligo a tutti gli Utenti di osservare il presente Disciplinare. Il mancato rispetto o la violazione delle regole in esso contenute è perseguibile nei confronti del personale dipendente con provvedimenti disciplinari previsti dai Contratti Collettivi Nazionali applicabili e nei confronti dei collaboratori e consulenti esterni, verificata la gravità della violazione contestata, con i rimedi contrattualmente previsti, inclusi la risoluzione od il recesso dal contratto, fermo restando i rimedi risarcitori e tutte le azioni civili e penali consentite esperibili nei confronti di qualsiasi trasgressore.

All'atto della sottoscrizione di un nuovo contratto individuale di lavoro ai nuovi assunti viene consegnata una copia del presente disciplinare da parte del Servizio Settore Risorse Umane. All'atto della sottoscrizione del contratto o dell'incarico di qualunque tipologia gli altri destinatari prendono visione del Disciplinare; a tal fine il Settore che ha condotto l'istruttoria legata alla definizione del contratto o dell'incarico medesimo comunica il link del sito internet istituzionale dove il medesimo è pubblicato

Allegato 1 - Atto di informazione ai sensi dell'art. 13 Regolamento UE 679/16 relativo al trattamento dei dati connessi all'utilizzo delle risorse e strumenti informatici

A norma dell'articolo 13 del Regolamento UE 679/16 ("Regolamento Generale sulla protezione dei dati", di seguito "GDPR"), ed in relazione al trattamento dei dati relativi all'utilizzo delle risorse e strumenti informatici aziendali da parte dei dipendenti/amministratori/collaboratori, il Comune di Vicenza (di seguito l'"Ente" o il "Titolare"), in qualità di titolare del trattamento, informa gli interessati di quanto segue.

1. Titolare del trattamento
Titolare del trattamento è il Comune di Vicenza, in persona del Sindaco, con sede in Corso Palladio n° 98, Vicenza, tel. 0444221111 - PEC vicenza@cert.comune.vicenza.it (di seguito anche solo il "Comune" o il "Titolare").

2. Dati di contatto del Responsabile della protezione dei dati
Il Comune di Vicenza ha nominato il Responsabile della protezione dei dati previsto dall'art. 37 GDPR (Data Protection Officer - DPO) reperibile ai seguenti contatti: e-mail dpo@comune.vicenza.it.

3. Finalità e base giuridica del trattamento
Il trattamento di dati personali connessi all'utilizzo delle Risorse ICT dell'Ente (es. nome e cognome dell'Utente, indirizzo IP, registrazione degli accessi in file log) avviene:

- per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio dell'Ente, compresa la sicurezza informatica e la tutela del sistema informatico aziendale, assistenza sistemistica, ecc., come specificato nel "Disciplinare istituzionale sull'utilizzo degli strumenti informatici e della posta elettronica" (di seguito il "Disciplinare");
- per effettuare controlli al fine di verificare il rispetto da parte degli Utenti delle regole previste nel Disciplinare;
- per la difesa dei diritti dell'Ente.

La base giuridica del trattamento è data dall'esecuzione del contratto di cui è parte l'Interessato (art. 6, par. 1 lett. b) GDPR) e dal perseguimento di un legittimo interesse del titolare del trattamento (art. 6, par. 1, lettera f) GDPR).

4. Natura del conferimento dei dati
Il conferimento dei dati personali è obbligatorio. In mancanza, all'Utente non sarà consentito l'utilizzo della strumentazione informatica di lavoro.

5. Modalità di trattamento e periodo di conservazione dei dati
I dati verranno trattati secondo le modalità descritte nel Disciplinare, e saranno protetti mediante adeguate misure di sicurezza di carattere fisico, logico e organizzativo. I dati personali saranno trattati da personale facente parte dell'organizzazione dell'Ente, dagli Amministratori di Sistema dell'Ente e da soggetti esterni designati quali responsabili del trattamento ai sensi dell'art. 28 GDPR. Non sono presenti processi automatizzati di profilazione.
I dati verranno conservati per il periodo specificato nel Disciplinare.

6. Destinatari dei dati

Gli indirizzi e-mail istituzionali nominativi potranno essere comunicati a dipendenti, utenti, fornitori e consulenti dell'Ente nell'ambito dell'ordinaria attività lavorativa.

I dati potranno essere comunicati all'Autorità Giudiziaria e/o all'Autorità di Pubblica Sicurezza e ad altri soggetti, nei casi previsti dalla legge o far valere in giudizio un diritto. I dati personali non saranno diffusi, fatta salva la pubblicazione degli indirizzi e-mail sul sito istituzionale dell'Ente.

I dati personali non saranno trasferiti a Paesi Terzi né ad organizzazioni internazionali.

7. Diritti dell'interessato

Ai sensi degli artt. 15-21 GDPR, gli Interessati hanno il diritto di:

- ottenere la conferma dell'esistenza o meno di un trattamento dei propri dati personali e in tal caso, di ottenere l'accesso ai dati ed alle informazioni di cui all'art. 15 GDPR (diritto di accesso);
- ottenere la rettifica dei dati personali inesatti senza ingiustificato ritardo o l'integrazione dei dati personali incompleti (diritto di rettifica - art. 16 GDPR);
- ottenere la cancellazione dei dati senza ingiustificato ritardo, ove applicabile (diritto alla cancellazione - art. 17 GDPR);
- ottenere la limitazione del trattamento (diritto di limitazione - art. 18 GDPR);
- opporsi al trattamento in qualsiasi momento per motivi connessi alla propria situazione particolare (diritto di opposizione - art. 21 GDPR).

I diritti possono essere esercitati contattando il DPO ai seguenti recapiti: dpo@comune.vincenza.it. Gli interessati possono altresì proporre reclamo al Garante per la Protezione dei Dati Personali ai sensi dell'art. 77 GDPR.

Allegato 2 - Atto di informazione ai sensi dell'art. 13 Regolamento UE 679/16 relativo al trattamento dei dati connessi allo svolgimento di riunioni/incontri in videoconferenza

A norma dell'articolo 13 del Regolamento UE 679/16 ("Regolamento Generale sulla protezione dei dati", di seguito "GDPR"), ed in relazione al trattamento dei dati connessi allo svolgimento di riunioni in videoconferenza, con eventuale registrazione delle sessioni, il Comune di Vicenza (di seguito l'"Ente" o il "Titolare"), in qualità di titolare del trattamento, informa gli interessati di quanto segue.

1. Titolare del trattamento
Titolare del trattamento è il Comune di Comune di Vicenza, in persona del Sindaco, con sede in Corso Palladio n° 98, Vicenza, tel. 0444221111 - PEC vicenza@cert.comune.vicenza.it (di seguito anche solo il "Comune" o il "Titolare").

2. Dati di contatto del Responsabile della protezione dei dati
Il Comune di Vicenza ha nominato il Responsabile della protezione dei dati previsto dall'art. 37 GDPR (Data Protection Officer - DPO) reperibile ai seguenti contatti: e-mail dpo@comune.vicenza.it.

3. Finalità e base giuridica del trattamento
Il trattamento di dati personali (es. nome e cognome, indirizzo e-mail del partecipante, immagini audio e video) avviene al solo scopo di permettere lo svolgimento di incontri/riunioni in modalità remota tra il personale dell'Ente e soggetti esterni o interni all'Ente, al fine di ottimizzare tempi e risorse e per necessità logistiche.
In caso di riunioni particolarmente tecniche o con un articolato ordine del giorno, l'Ente può procedere alla registrazione della sessione, al fine di agevolare le attività di verbalizzazione o stesura della minuta dell'incontro. In questo caso, l'organizzatore della riunione è tenuto a comunicare ai partecipanti, prima dell'inizio della riunione, l'avvio della registrazione, dando piena informativa sul trattamento dati.
La base giuridica del trattamento è data dall'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri (art. 6. par. 1, lettera e) GDPR e art. 2 ter d.lgs. 196/2003).

4. Natura del conferimento dei dati
Il conferimento dei dati personali è obbligatorio ai fini della partecipazione della riunione, ad eccezione delle immagini video, per le quali è facoltà del partecipante attivare o meno la telecamera, salvo la necessità di identificare previamente i partecipanti.

5. Modalità di trattamento e periodo di conservazione dei dati
I dati verranno protetti mediante adeguate misure di sicurezza di carattere fisico, logico e organizzativo. I dati personali saranno trattati da personale facente parte dell'organizzazione dell'Ente, dagli Amministratori di Sistema dell'Ente e da soggetti esterni designati quali responsabili del trattamento ai sensi dell'art. 28 GDPR. Non sono presenti processi automatizzati di profilazione. L'eventuale registrazione verrà conservata per il tempo strettamente necessario per la gestione dell'istruttoria/procedimento inerente alla riunione, dopodichè verrà cancellata da ogni supporto.

6. Destinatari dei dati
I dati personali potranno essere comunicati ai partecipanti all'incontro e al gestore della

piattaforma, quale responsabile del trattamento, al solo fine dell'esecuzione della videoconferenza. La registrazione delle riunioni potrà essere trasmessa al personale dell'Ente coinvolto nel procedimento inerente all'incontro per i soli fini istituzionali.
I dati potranno essere comunicati all'Autorità Giudiziaria e/o all'Autorità di Pubblica Sicurezza, nei casi previsti dalla legge o per far valere in giudizio un diritto. I dati personali non saranno diffusi né trasferiti a Paesi Terzi né ad organizzazioni internazionali.

7. Diritti dell'interessato
Ai sensi degli artt. 15-21 GDPR, gli Interessati hanno il diritto di:

- ottenere la conferma dell'esistenza o meno di un trattamento dei propri dati personali e in tal caso, di ottenere l'accesso ai dati ed alle informazioni di cui all'art. 15 GDPR (diritto di accesso);
- ottenere la rettifica dei dati personali inesatti senza ingiustificato ritardo o l'integrazione dei dati personali incompleti (diritto di rettifica - art. 16 GDPR);
- ottenere la cancellazione dei dati senza ingiustificato ritardo, ove applicabile (diritto alla cancellazione - art. 17 GDPR);
- ottenere la limitazione del trattamento (diritto di limitazione - art. 18 GDPR);
- opporsi al trattamento in qualsiasi momento per motivi connessi alla propria situazione particolare (diritto di opposizione - art. 21 GDPR).

I diritti possono essere esercitati contattando il DPO ai seguenti recapiti: dpo@comune.vincenza.it. Gli interessati possono altresì proporre reclamo al Garante per la Protezione dei Dati Personali ai sensi dell'art. 77 GDPR.