Comune di Rubano
Provincia di Padova

REGOLAMENTO PER L'UTILIZZO DELLA STRUMENTAZIONE INFORMATICA, TELEMATICA E TELEFONICA

Approvato con delibera G.C. 137 del 22.12.2021

Art. 1 - PREMESSA

1. La progressiva diffusione delle tecnologie, ed il necessario utilizzo della rete informatica, potrebbe esporre l'Ente e gli utenti (meglio specificati in seguito) a rischi di carattere patrimoniale oltre a responsabilità penali conseguenti alla violazione di specifiche disposizioni di legge (ad. esempio legge sulla privacy) con ricadute negative in termini di sicurezza e di immagine dell'Azienda stessa.
2. Il presente Disciplinare si propone di stabilire modalità e finalità di utilizzo dei beni dell'ente, regolando le condizioni per il corretto utilizzo degli strumenti informatici, telematici e telefonici da parte degli utenti.

Art. 2 - DESTINATARI

1. Sono tenuti ad osservare il presente disciplinare tutti gli utilizzatori di strumenti informatici, telematici e telefonici di proprietà del Comune di Rubano, a prescindere dal tipo di rapporto sulla cui base ne fanno uso.
2. Sono quindi tenuti ad osservarlo i dipendenti, gli amministratori, i lavoratori somministrati, i lavoratori socialmente utili, i lavoratori di pubblica utilità, e gli altri soggetti a cui siano affidati strumenti informatici, telematici e telefonici di proprietà del Comune di Rubano.

Art. 3 – PRINCIPI E REGOLE GENERALI

1. Le risorse informatiche e telematiche dell'Ente devono ispirarsi ai principi di diligenza, correttezza e buona fede (principi questi che sono comunque sottesi al rapporto di lavoro). La stesura del presente disciplinare è stata formulata sulla base delle linee guida emanate dall'Autorità Garante per la Protezione dei Dati Personali, con propria deliberazione n. 13 del 1° marzo 2007, sulla disciplina della navigazione in internet e sulla gestione della posta elettronica nei luoghi di lavoro nonché alle sulla base delle misure tecniche e organizzative adeguate alla valutazione del rischio specifico in azienda, come stabilito dal nuovo Regolamento Europeo GDPR 2016/679.
2. La regolamentazione degli strumenti e delle risorse informatiche-telematiche-telefoniche deve garantire il diritto del datore di lavoro di proteggere la propria organizzazione, salvaguardando il diritto del lavoratore a non vedere invasa la propria sfera personale.
3. Agli utilizzatori delle strumentazioni informatiche, telematiche e telefoniche inventariate si applicano le disposizioni contenute nell'art. 40, comma 5, del regolamento comunale di contabilità, in quanto svolgono di fatto la funzione di sub-agenti consegnatari di beni comunali.

Art. 4. - UTILIZZO DEL PERSONAL COMPUTER

1. Il Personal Computer affidato all'utente è uno strumento di lavoro. Ogni utilizzo non inerente all'attività lavorativa è vietato perché può contribuire ad innescare disservizi, costi di manutenzione e,

soprattutto, minacce alla sicurezza. Il personal computer deve essere custodito con cura evitando ogni possibile forma di danneggiamento.
2. Il personal computer affidato all'utente permette l'accesso alla rete solo attraverso specifiche credenziali di autenticazione.
3. L'ente rende noto che il personale tecnico interno ed esterno (appositamente incaricato) è autorizzato a compiere interventi nel sistema informatico diretti a garantire la sicurezza e la salvaguardia del sistema stesso, nonché per ulteriori motivi tecnici e/o manutentivi (ad es. aggiornamento / sostituzione/implementazione di programmi, manutenzione hardware, ecc...). Detti interventi potranno anche comportare l'accesso in qualunque momento ai dati trattati da ciascuno, ivi compresi gli archivi di posta elettronica, nonché alla verifica sui siti visitati dagli utenti.
4. La stessa facoltà, sempre ai fini della sicurezza del sistema e per garantire la normale operatività dell'ente, si applica anche in caso di assenza prolungata o impedimento dell'utente.
5. Si prevede che l'attività su internet dei singoli utenti venga registrata in appositi log mantenuti dai Sistemi Informativi e regolata da appositi filtri di navigazione. Questi ultimi sono implementati mediante uno specifico software, che opera congiuntamente a un sistema web gateway, per finalità di tutela e per poter eventualmente riferire all'Autorità Giudiziaria comportamenti anomali registrati dai sistemi. In tal modo l'Ente intende prevenire il libero accesso ai siti presenti in rete da parte della generalità dei lavoratori, confinandolo ai soli siti web ritenuti conferenti con lo svolgimento delle attività lavorative (salva diversa valutazione da effettuarsi caso per caso).
6. La gestione dei Log è in carico all'Ente che li tratterà secondo le normative vigenti. Il personale incaricato del servizio IT ha la facoltà di collegarsi e visualizzare in remoto il desktop delle singole postazioni PC al fine di garantire l'assistenza tecnica e la normale attività operativa, nonché la massima sicurezza contro virus, spyware, malware, ecc... L'intervento viene effettuato esclusivamente su chiamata dell'utente o, in caso di oggettiva necessità, a seguito della rilevazione tecnica di problemi nel sistema informatico. In quest'ultimo caso, sempre che non si pregiudichi la necessaria tempestività ed efficacia dell'intervento, verrà data comunicazione della necessità dell'intervento stesso.
7. Non è consentito l'uso di programmi diversi da quelli ufficialmente installati, né viene consentito agli utenti di installare autonomamente programmi provenienti dall'esterno, sussistendo infatti il grave pericolo di introdurre virus informatici e/o di alterare la funzionalità delle applicazioni software esistenti. Si evidenzia che le violazioni della normativa a tutela dei diritti d'autore sul software che impone la presenza nel sistema di software regolarmente licenziato, o comunque libero e quindi non protetto dal diritto d'autore, sono sanzionabili anche penalmente. E' presente nel sistema un software per la gestione degli applicativi sui client, con la possibilità di generare un report puntuale, contenente i software installati su ogni singolo client a scopo di controllo anonimo/difensivo.
8. Salvo preventiva espressa autorizzazione, non è consentito all'utente modificare le caratteristiche impostate sul proprio PC, né procedere ad installare dispositivi di memorizzazione, comunicazione o altro (come ad esempio: masterizzatori, chiavette wi-fi o bluetooth, ecc…).
9. In ogni caso, ogni utente deve prestare la massima attenzione ai supporti di origine esterna (come ad esempio: chiavette usb, hard disk esterni, ecc…), preventivamente autorizzati, avvertendo immediatamente il personale del Servizio IT nel caso in cui siano stai rilevati virus ed adottando quanto previsto nelle procedure di protezione antivirus.
10. Il Personal Computer deve essere spento ogni sera prima di lasciare gli uffici o in caso di assenze prolungate dall'ufficio o in caso di suo inutilizzo. In ogni caso, lasciare un elaboratore 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.

Art. 5 - ULTERIORI REGOLE IN CASO DI UTILIZZO DI PC E DISPOSITIVI PORTATILI

1. L'utilizzo di strumenti "mobili" quali PC portatili, smartphone e tablet, comporta ulteriori rischi per l'utilizzatore, in quanto si rendono molto più probabili eventi quali furto, smarrimento, rottura (per caduta, trasporto, ecc) o utilizzo da parte di terzi non autorizzati.
2. Tutti gli strumenti portatili dati in uso sono strumenti di proprietà del Comune di Rubano e sono destinati esclusivamente ad un uso professionale. L'utente si impegna quindi, sotto la propria responsabilità, ad assicurarne l'uso esclusivamente per scopi di lavoro e si impegna altresì a prevenirne l'uso da parte di terzi (familiari, amici, ecc).

3. I dispositivi mobili consegnati sono dotati di strumenti per la crittazione dei dati, in caso di smarrimento o furto non sarà possibile comunque a terzi l'accesso ai dati in essi contenuti.
4. In caso di smarrimento, furto o guasto, l'utente è tenuto a darne immediata comunicazione al team IT affinché vengano messe in opera tutte le attività di emergenza per il blocco degli accessi alla rete del Comune.
5. I PC portatili sono dotati di accesso VPN securizzato alla rete del Comune, l'utente dovrà porre particolare attenzione a non salvare o lasciare traccia delle credenziali di accesso VPN.
6. Poiché i dispositivi portatili vengono connessi a reti dati non gestite o controllate dal Comune (rete WIFI domestica o reti presenti in luoghi nei quali l'utente opera quando non è in ufficio), l'utente deve prestare la massima cura ed attenzione, evitando l'accesso a reti "aperte" e/o pubbliche, nelle quali non è garantito l'isolamento del client.

Art. 6 - GESTIONE ED ASSEGNAZIONE DELLE CREDENZIALI DI AUTENTICAZIONE

1. Le credenziali di autenticazione per l'accesso alla rete vengono assegnate dal personale del Servizio IT, previa formale richiesta del Responsabile dell'ufficio / area nell'ambito del quale verrà inserito ed andrà ad operare il nuovo utente.
2. Le credenziali di autenticazione consistono in un codice per l'identificazione dell'utente (user id), associato ad una parola chiave (password) riservata che dovrà essere custodita dall'incaricato con la massima diligenza e non divulgata. Non è consentita l'attivazione della password di accensione (bios).
3. La parola chiave, per buona norma, deve essere formata da lettere (maiuscole o minuscole) e/o numeri, anche in combinazione fra loro, deve essere composta da almeno otto caratteri e non deve contenere riferimenti agevolmente riconducibili al titolare. È necessario procedere alla modifica della parola chiave a cura dell'utente, incaricato del trattamento, al primo utilizzo e, successivamente, ogni tre mesi.
4. Qualora la parola chiave dovesse venir sostituita per decorso del termine sopra previsto e/o in quanto abbia perduto la propria riservatezza, si procederà in tal senso d'intesa con il personale incaricato.

Art. 7 - UTILIZZO DELLA RETE DELL'ENTE

1. Per l'accesso alla rete dell'Ente ciascun utente deve essere in possesso della specifica credenziale di autenticazione. È assolutamente proibito entrare nella rete e nei programmi con un codice d'identificazione utente diverso da quello assegnato. Le credenziali d'ingresso alla rete ed ai programmi sono segrete e vanno comunicate e gestite secondo le procedure impartite.
2. Le cartelle utenti presenti nei server sono aree di condivisione di informazioni strettamente professionali e non possono in alcun modo essere utilizzate per scopi diversi. Pertanto qualunque file che non sia legato all'attività lavorativa non può essere dislocato, nemmeno per brevi periodi, in queste unità. In particolare, nelle cartelle di rete sarà controllata la presenza di: categorie di file non permessi, file di grandi dimensioni e file non pertinenti.
3. Risulta opportuno che, con regolare periodicità (almeno ogni tre mesi), ciascun utente provveda alla pulizia degli archivi, con cancellazione dei file obsoleti o inutili. Particolare attenzione deve essere prestata alla duplicazione dei dati, essendo, infatti, necessario evitare un'archiviazione ridondante.
4. Si fa obbligo di salvataggio nei percorsi di rete pertinenti a seconda della tipologia di dato/file e del suo contenuto.

Art. 8 - UTILIZZO E CONSERVAZIONE DEI SUPPORTI RIMOVIBILI

1. Tutti i supporti rimovibili autorizzati (CD e DVD riscrivibili, supporti USB, hard disk esterni, memorie flash, ecc.) contenenti dati riservati nonché informazioni costituenti know-how aziendale, devono essere trattati con particolare cautela onde evitare che il loro contenuto possa essere trafugato, alterato, distrutto o, successivamente alla cancellazione, recuperato. In ogni caso, i supporti magnetici contenenti dati riservati devono essere adeguatamente custoditi in armadi chiusi dagli utenti. E' vietato l'utilizzo di supporti rimovibili personali. L'utente è responsabile della custodia dei supporti e dei dati aziendali in essi contenuti.

Art. 9 - GESTIONE E UTILIZZO DELLA POSTA ELETTRONICA

1. La casella di posta elettronica assegnata all'utente è uno strumento di lavoro è quindi destinata esclusivamente all'utilizzo professionale.
2. Si fa presente inoltre che: non è consentito inviare o memorizzare messaggi (interni ed esterni) di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica, o che costituiscano comunque condotta illecita.
3. Non è consentito l'utilizzo dell'indirizzo di posta elettronica per la partecipazione a dibattiti, Forum, newsletter o mail-list, non attinenti l'attività lavorativa.
4. In caso di assenza, al dipendente sono posti a disposizione apposite funzioni di sistema che consentano di inviare automaticamente messaggi di risposta.
5. E' vietato divulgare le notizie, i dati e qualsiasi altra informazione appresa in occasione della ricezione o invio di posta elettronica, in quanto coperte dal segreto professionale cui sono tenuti i dipendenti in ottemperanza agli obblighi di fedeltà e correttezza.
6. La posta elettronica diretta all'esterno della rete informatica aziendale può essere intercettata da estranei e, dunque, è preferibile non usarla per inviare documenti di lavoro "Strettamente Riservati".
7. In caso di assenza programmata, sarà attivata dall'utente la risposta automatica di assenza con indicazioni per il reinvio verso caselle presidiate.
8. E' vietato divulgare le notizie, i dati e qualsiasi altra informazione appresa in occasione della ricezione o invio di posta elettronica, in quanto coperte dal segreto professionale cui sono tenuti gli utenti in ottemperanza agli obblighi di fedeltà e correttezza.
9. E' buona norma rispondere ad e-mail pervenute solo da mittenti conosciuti e cancellare preventivamente le altre.
10. Non è consigliabile collegarsi a siti internet linkati all'interno di messaggi.
11. E' necessario mantenere in ordine la casella di posta, secondo le istruzioni ricevute.

Art. 10 – ACCESSO ALLA CASELLA DI POSTA IN CASO DI ASSENZA DELL'UTENTE

1. In caso di eventuali assenze non programmate (ad es., per malattia), l'ente, perdurando l'assenza oltre un determinato limite temporale pari a 2 giorni, potrà disporre lecitamente, sempre che sia necessario per esigenze organizzative segnalate dal responsabile di servizio, e mediante personale appositamente incaricato alla variazione della password attraverso l'autorizzazione del titolare o incaricato preposto; di tale attività sarà informato l'utente interessato alla prima occasione utile.

Art. 11 – CHIUSURA DELLA CASELLA DI POSTA ELETTRONICA

1. In caso di cessazione del rapporto di lavoro con l'utente, l'accesso all'indirizzo di posta elettronica verrà disabilitato alla data di fine rapporto di lavoro; la posta in entrata verrà reindirizzata ad un altro indirizzo di posta aziendale presidiato; entro 6 mesi, invece, si disporrà la definitiva e totale cancellazione dello stesso.
2. L'ente si riserva il diritto di conservare i messaggi di posta elettronica che riterrà rilevanti, su valutazione del responsabile di servizio.

Art. 12 - NAVIGAZIONE IN INTERNET

1. Il PC assegnato al singolo utente ed abilitato alla navigazione in internet costituisce uno strumento utilizzabile esclusivamente per lo svolgimento della propria attività lavorativa. È quindi assolutamente proibita la navigazione in Internet per motivi diversi da quelli strettamente legati all'attività lavorativa.
2. In questo senso, a titolo puramente esemplificativo, l'utente non potrà utilizzare Internet per: l'upload o il download di software gratuiti (freeware) e shareware, nonché l'utilizzo di documenti provenienti da siti web o http, se non strettamente attinenti all'attività lavorativa (filmati e musica) e previa verifica dell'attendibilità dei siti in questione; l'effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti on-line e simili, e comunque nel rispetto delle normali procedure di acquisto; ogni forma di registrazione a siti i cui contenuti non siano strettamente legati all'attività lavorativa; la partecipazione a Forum non professionali, l'utilizzo di chat line (esclusi gli strumenti autorizzati), di bacheche elettroniche e le registrazioni in guest books anche utilizzando pseudonimi (o nicknames) se non espressamente autorizzati dal Responsabile di servizio; l'accesso, tramite internet, a caselle webmail di posta elettronica personale.

Art. 13 - PROTEZIONE ANTIVIRUS

1. Il sistema informatico è protetto da software antivirus aggiornato quotidianamente. Ogni utente deve comunque tenere comportamenti tali da ridurre il rischio di attacco al sistema informatico mediante virus o mediante ogni altro software aggressivo. Nel caso il software antivirus rilevi la presenza di un virus, l'utente dovrà immediatamente sospendere ogni elaborazione in corso, nonché segnalare prontamente l'accaduto al personale del Servizio IT.

Art. 14 - UTILIZZO DI TELEFONI, FAX E FOTOCOPIATRICI

1. Il telefono aziendale affidato all'utente è uno strumento di lavoro. Ne viene concesso l'uso esclusivamente per lo svolgimento dell'attività lavorativa, non essendo quindi consentite comunicazioni a carattere personale o comunque non strettamente inerenti l'attività lavorativa stessa.
2. E' vietato l'utilizzo dei fax aziendali per fini personali, tanto per spedire quanto per ricevere documentazione, salva diversa esplicita autorizzazione da parte del responsabile di ufficio.
3. In caso di stampe contenenti dati sensibili e riservati, l'utente dovrà porre in essere tutte le attenzioni affinche' il documento stampato non possa essere visionato o prelevato da terzi.
4. E' vietato l'invio di scansioni con dati sensibili aziendali su dischi comuni.
5. E' vietato l'utilizzo delle fotocopiatrici aziendali per fini personali, salvo preventiva ed esplicita autorizzazione da parte del responsabile di servizio.

Art. 15 - OSSERVANZA DELLE DISPOSIZIONI IN MATERIA DI PRIVACY

1. È obbligatorio attenersi alle disposizioni in materia di Privacy e alle pertinenti e adeguate misure di sicurezza ai sensi del Regolamento Europeo GDPR EU 2016/679, oltre che alle istruzioni impartite in occasione dell'autorizzazione al trattamento dei dati personali.

Art. 16 - ACCESSO AI DATI TRATTATI DALL'UTENTE

1. E' facoltà dell'Ente, tramite il personale del Servizio IT, nel pieno rispetto della normativa sulla privacy, accedere a tutti gli strumenti informatici aziendali e ai documenti ivi contenuti per motivi di sicurezza del sistema informatico, per motivi tecnici e/o manutentivi (ad esempio, aggiornamento/sostituzione/implementazione di programmi, manutenzione hardware, ecc...), per finalità di controllo e programmazione dei costi aziendali (ad esempio, verifica costi di connessione ad Internet, traffico telefonico, ecc...), nonché ai tabulati del traffico telefonico. Tali attività non hanno la finalità di controllo sull'attività lavorativa individuale.

Art. 17 – CONTROLLI

1. Il Garante per la protezione dei dati personali ha emesso un provvedimento in cui ha fornito le linee guida che bilanciano due diverse esigenze: il diritto di controllo da parte del datore di lavoro circa le modalità di utilizzo degli strumenti informatici, con particolare riferimento a servizi di e-mail ed accesso ad Internet, messi a disposizione degli incaricati, ed il diritto di questi ultimi a non subire intrusioni illecite nella propria sfera privata.
2. Il presente documento deve essere considerato come integrazione dell'autorizzazione e delle istruzioni aventi ad oggetto i criteri e le modalità operative di accesso ed utilizzo del servizio internet e di posta elettronica da parte degli addetti.
3. Restano ferme, ove non espressamente modificate nel presente documento, tutte le indicazioni del Titolare del trattamento e del Responsabile del trattamento.
4. Eventuali controlli escludono finalità di monitoraggio diretto ed intenzionale dell'attività lavorativa e sono disposti sulla base della vigente normativa, con particolare riferimento alla Legge n. 300/1970 (c.d. Statuto dei Lavoratori) ed ai provvedimenti appositamente emanati dall'Autorità Garante. L'Ente esclude la configurabilità di forme di controllo aziendali aventi direttamente ad oggetto l'attività lavorativa dell'Utente.
5. Non si esclude che, per ragioni organizzative e produttive, di protezione dei dati ovvero per esigenze dettate dalla sicurezza del lavoro, si utilizzino sistemi informatici, impianti o apparecchiature dai quali derivi la possibilità di controllo dell'attività lavorativa.
6. L'ente, nel riservarsi il diritto di procedere a tali controlli sull'effettivo adempimento della prestazione lavorativa nonché sull'utilizzo da parte degli utenti dei beni e dei servizi informatici aziendali (artt. 2086,

2087 e 2104 c.c.), agirà in base al principio della “gradualità”, quindi: i controlli saranno effettuati inizialmente solo su dati aggregati riferiti all’intera struttura aziendale o a specifiche aree lavorative; nel caso in cui si dovessero riscontrare anomalie, indizi di commissione di gravi abusi o illeciti o attività contrarie ai doveri di fedeltà e diligenza, verrà diffuso un avviso generalizzato, o circoscritto all’area o struttura lavorativa interessata, con conseguente invito ad attenersi scrupolosamente alle istruzioni impartite; in caso siano rilevate ulteriori violazioni, si potrà procedere con verifiche più specifiche e puntuali, anche su base individuale.

7. Con riguardo al principio secondo cui occorre perseguire finalità determinate, esplicite e legittime, il datore di lavoro può riservarsi di controllare direttamente o attraverso la propria struttura l'effettivo adempimento della prestazione lavorativa e, se necessario, il corretto utilizzo degli strumenti di lavoro (cfr. artt. 2086, 2087 e 2104 cod. civ.). Nell'esercizio di tale prerogativa occorre rispettare la libertà e la dignità dei lavoratori, in particolare per ciò che attiene alle regole per l’installazione di apparecchiature che possano anche attivare finalità di controllo a distanza dell'attività dei lavoratori (art. 4, l. n. 300/1970 così come aggiornata nel settembre 2015), tra cui sono certamente comprese strumentazioni hardware e software mirate al controllo dell'utente di un sistema di comunicazione elettronica.

8. Per queste ragioni è assolutamente proibito a chiunque ogni trattamento effettuato mediante sistemi hardware e software preordinati al controllo a distanza grazie ai quali sia possibile ricostruire, a volte anche minuziosamente, l’attività dei lavoratori. E’ il caso, ad esempio: della lettura e della registrazione sistematica dei messaggi di posta elettronica ovvero dei relativi dati esteriori, al di là di quanto tecnicamente necessario per svolgere il servizio e-mail; della riproduzione ed eventuale memorizzazione sistematica delle pagine web visualizzate dal lavoratore; della lettura e della registrazione dei caratteri inseriti tramite la tastiera o analogo dispositivo; dell'analisi occulta di computer portatili affidati in uso.

6. L’ente - utilizzando sistemi informativi per esigenze produttive o organizzative (ad es. per rilevare anomalie o per manutenzioni) o, comunque, quando gli stessi si rivelano necessari per la sicurezza sul lavoro - può avvalersi legittimamente, nel rispetto dello Statuto dei lavoratori di sistemi che consentono indirettamente un controllo a distanza (c.d. controllo preterintenzionale) e determinano un trattamento di dati personali riferiti o riferibili ai lavoratori.

9. L’ente promuove ogni opportuna misura, organizzativa e tecnologica volta a prevenire il rischio di utilizzi impropri (da preferire rispetto all'adozione di misure "repressive", come suggerisce il Garante) e, comunque, a "minimizzare" l'uso di dati riferibili ai lavoratori.

10. Per questo, dal punto di vista organizzativo, l’ente ha valutato e valuterà attentamente l'impatto sui diritti dei lavoratori prima dell'installazione di apparecchiature suscettibili di consentire il controllo a distanza e dell'eventuale trattamento.

11. In caso di anomalie, il personale incaricato del servizio IT effettuerà controlli anonimi che si concluderanno con un avviso generalizzato diretto ai dipendenti dell’area o del settore in cui è stata rilevata l’anomalia, nei quali si evidenzierà l’utilizzo irregolare degli strumenti aziendali e si inviteranno gli interessati ad attenersi scrupolosamente ai compiti assegnati e alle istruzioni impartite.

12. Attraverso il Log di Sistema, il sistema registra informazioni sui siti web visitati e sulla quantità di byte scaricati o inviati. Il file di log contiene per ogni accesso: l’indirizzo web del sito visitato, data ora minuti e secondi. Il file di log viene registrato senza alcun riferimento diretto all’utente che ha effettuato le operazioni. Solo con eventuali successive operazioni di comparazione è possibile risalire all’utente specifico.

I file di log vengono conservati per un periodo di 186 giorni.

13. Il Log consente l’estrazione di dati statistici che possono evidenziare anomalie (accesso a siti non autorizzati, utilizzi non moderati del download, ecc.) che possono portare a verifiche per gruppi ampi di utenti, sui quali compiere le dovute azioni di avviso.

14. Nessuno è autorizzato a verificare il contenuto dei file di log della navigazione in internet, fatti salvi i controlli di cui al punto 14 e, naturalmente, per verifiche e indagini richieste dalle autorità.

15. Il servizio mail è esternalizzato alla Provincia di Padova: il Comune non può pertanto effettuare controlli diretti e specifici. Per le informazioni specifiche relative all’erogazione del servizio di posta elettronica si rimanda alla documentazione della Provincia disponibile al link http://cst.provincia.padova.it.

16. Gli unici soggetti preposti al controllo operativo degli ambienti di posta elettronica e di internet sono gli Amministratori di Sistema, i quali, appositamente incaricati, agiscono con la supervisione del Titolare.

Ai soggetti preposti corre l'obbligo di svolgere solo operazioni strettamente necessarie al perseguimento delle finalità riconducibili alla ricerca e all'esame di situazioni anomale e alle attività di manutenzione dei Sistemi.

17. E' proibito a soggetti privi dello specifico incarico da parte dell'ente di effettuare qualunque genere di attività finalizzate al controllo sulla posta elettronica e sull'accesso a Internet, anche per perseguire finalità lecite. In ogni caso, qualora necessario, i controlli saranno comunque effettuati da un numero limitato di persone.

18. L'eventuale controllo sulla posta elettronica e sull'accesso a Internet è lecito solo se sono rispettati i principi di pertinenza e non eccedenza. Nel caso in cui un evento dannoso o una situazione di pericolo non sia stato impedito con preventivi accorgimenti tecnici, l'ente adotta misure che consentano la verifica di comportamenti anomali.

19. Chiunque tra il personale dipendente o collaboratore può segnalare un'anomalia circa la navigazione web o l'uso della Posta Elettronica. La segnalazione va inoltrata al Titolare e al Responsabile del Trattamento dei dati personali.

20. Il controllo aggregato, di sua natura anonimo, può concludersi con un avviso generalizzato relativo ad un rilevato utilizzo anomalo degli strumenti aziendali e con l'invito ad attenersi scrupolosamente a compiti assegnati e istruzioni impartite. L'avviso può essere circoscritto ad incaricati afferenti all'area o settore in cui è stata rilevata l'anomalia.

21. Se dopo gli opportuni controlli collettivi e i relativi avvisi, l'anomalia si ripete, possono essere effettuati controlli su base individuale, nominativi, sui singoli dispositivi e postazioni. Deve essere inoltrato, con la dovuta riservatezza, un preventivo avviso individuale alla persona oggetto del controllo con espresse le ragioni legittime della verifica e le modalità tecniche con cui verrà effettuata.

22. L'ente, in ottica di quanto precedentemente definito, nel caso constati che la posta elettronica e la rete internet sono utilizzate indebitamente, può intervenire disciplinarmente nei confronti dell'utente applicando il sistema sanzionatorio in vigore. Rimane salva la denuncia all'autorità costituita qualora il comportamento costituisca reato.