Marianna Chinellato
Avvocato

Arcangelo Ceci
Dott. Commercialista

Mauro Badalin
Business Advisor

Domenico Nastari
Avvocato

Daniele Epifani
Dott. Commercialista

Jessica Andreetta
Consulente Aziendale

Regolamento per l'utilizzo degli strumenti informatici aziendali

1 dicembre

2017

Rev. 1.0

Policies

Sede legale e operativa: via Terraglio, 263/A - 31022 Preganziol (TV) - tel. 0422 633.882 - fax 0422 633.881
Sede operativa: via Einaudi, 62 - 31074 Mestre (VE) - tel. 041 961.624 - fax 041 954.958
C.F. / P.IVA: 03690390269 - e-mail: consulting@hunext.com - PEC: hunext.consulting@legalmail.it - www.hunext.com

Marianna Chinellato
Avvocato

Arcangelo Ceci
Dott. Commercialista

Mauro Badalin
Business Advisor

Domenico Nastari
Avvocato

Daniele Epifani
Dott. Commercialista

Jessica Andreetta
Consulente Aziendale

Sommario

Premessa 3
1. Entrata in vigore del Regolamento e pubblicità 4
2. Principi generali di riservatezza nelle comunicazioni 5
3. Trattamenti con Strumenti elettronici 6
5. Controlli sugli strumenti (art. 6.1 Provv. Garante, ad integrazione dell'informativa ex art. 13 d.lgs 196/03) 15
6. Partecipazioni a social media 17
7. Sanzioni 18
8. Aggiornamento e revisione 19

Premessa

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

Ogni dipendente e collaboratore è tenuto a rispettare il Regolamento, che è reso disponibile secondo quanto previsto al successivo punto 1.3.

Si specifica che tutti gli strumenti utilizzati dal lavoratore (hardware, software, risorse, e-mail ecc.) sono messi a disposizione dal Consorzio per rendere la prestazione lavorativa. Gli Strumenti, nonché le relative reti dell'Ente a cui è possibile accedere tramite gli Strumenti, sono domicilio informatico del Consorzio di Bonifica Chiese.

I dati personali e le altre informazioni dell'Utente che sono registrati negli Strumenti o che si possono eventualmente raccogliere dall'uso degli Strumenti, sono utilizzate per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale. Per tutela del patrimonio aziendale si intende altresì la sicurezza informatica e la tutela del sistema informatico aziendale. Tali informazioni sono altresì utilizzabili a tutti i fini connessi al rapporto di lavoro, visto che il presente Regolamento costituisce adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli, sempre nel rispetto di quanto disposto dal Decreto Legislativo 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali".

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

Il presente Regolamento è adottato ai sensi dell'art. 4 comma 3 della L. 300/70 e delle "Linee guida del Garante per posta elettronica e internet" in Gazzetta Ufficiale n. 58 del 10 marzo 2007 ed integra l'informativa sul trattamento dei dati personali resa ai sensi dell'art. 13 del D.lgs 196/03.

1. Entrata in vigore del Regolamento e pubblicità

1.1 Il presente Regolamento entra in vigore il 01 dicembre 2017.

1.2 Con l'entrata in vigore del presente Regolamento tutte le norme e le disposizioni in precedenza adottate in materia, in qualsiasi forma comunicate, devono intendersi abrogate e sostituite dalle presenti.

1.3 Copia del Regolamento, oltre ad essere affisso nella bacheca consortile, è reso disponibile presso l'Ufficio Amministrativo.

2. Principi generali di riservatezza nelle comunicazioni

2.1. Il dipendente si attiene alle seguenti regole di trattamento.

a) È vietato comunicare a soggetti non specificatamente autorizzati i dati personali comuni, sensibili, giudiziari, sanitari o altri dati, elementi e informazioni aziendali dei quali il dipendente / collaboratore viene a conoscenza nell'esercizio delle proprie funzioni e mansioni all'interno dell'Ente. In caso di dubbio, è necessario accertarsi che il soggetto cui devono essere comunicati i dati sia o meno autorizzato a riceverli, mediante richiesta preventiva al proprio Responsabile di Area/Settore.

b) È vietata l'estrazione di originali e/o copie cartacee ed informatiche per uso personale di documenti, manuali, fascicoli, lettere, data base e quant'altro.

c) È vietato effettuare colloqui con utenti o colleghi su questioni che possono essere inerenti informazioni o dati personali in presenza di persone non specificatamente incaricate a conoscere tali informazioni. Nelle ipotesi in cui siano presenti dette persone non incaricate, è necessario interrompere la comunicazione, riprendendola in luogo diverso e più riservato o attendere che i soggetti estranei non siano più presenti.

d) È vietato lasciare incustoditi documenti, lettere, fascicoli, appunti e quant'altro possa contenere dati personali e/o informazioni aziendali quando il dipendente/collaboratore si allontana dalla postazione di lavoro.

3. Trattamenti con Strumenti elettronici

3.1. Per "strumenti elettronici" si intendono i PC, notebook, tablet, smartphone e altri strumenti con relativi software e applicativi (di seguito anche "Strumenti") utilizzati per rendere la prestazione lavorativa che sono di proprietà del Consorzio, salvo diverso accordo con il lavoratore.

Il dipendente/collaboratore è consapevole che gli Strumenti forniti sono di proprietà del Consorzio di Bonifica Chiese e devono essere utilizzati esclusivamente per rendere la prestazione lavorativa.

Ciascun dipendente /collaboratore si deve attenere alle seguenti regole di utilizzo degli Strumenti.

a) Gli Strumenti affidati all'incaricato sono uno strumento di lavoro di proprietà dell'Ente. Ogni utilizzo degli stessi non inerente all'attività lavorativa è vietato perché può contribuire ad innescare disservizi, costi di manutenzione e minacce alla sicurezza.
b) Il Personal Computer, notebook, tablet ed ogni altro hardware deve essere custodito con cura da parte degli assegnatari evitando ogni possibile forma di danneggiamento e segnalando tempestivamente al responsabile informatico ogni malfunzionamento e/o danneggiamento.
c) Il Personal Computer deve essere spento al termine della giornata lavorativa oppure se ci si assenta dall'ufficio per un periodo di tempo prolungato. Negli altri casi di inutilizzo, anche se per brevi periodi, è comunque necessario disconnetterlo dalla rete premendo i tasti ctrl+alt+canc.
d) Non devono essere lasciati lavori incompiuti sullo schermo. È buona norma non lasciare documenti aperti e visibili sullo schermo del PC quando vi allontanate dalla postazione di lavoro anche solo temporaneamente o quando si riceve il pubblico, clienti/fornitori o colleghi.
e) È vietato l'utilizzo di supporti di memoria (chiavi USB, CD, DVD o altri supporti) per il salvataggio di dati trattati tramite gli strumenti Aziendali, salvo che il supporto utilizzato sia stato fornito dal responsabile informatico. In tale caso, il supporto fornito può essere utilizzato esclusivamente per finalità lavorative.
f) Gli Strumenti sono accessibili esclusivamente attraverso specifiche credenziali di autenticazione come meglio descritto al successivo punto 5 del presente Regolamento.
g) Non deve essere permesso l'uso del proprio Strumento e/o account ad altri colleghi d'ufficio o a soggetti terzi.
h) Non è consentito l'uso di programmi diversi da quelli ufficialmente installati dal responsabile informatico per conto del Consorzio di Bonifica Chiese, 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. L'inosservanza della presente disposizione espone il Consorzio di Bonifica Chiese a gravi responsabilità civili; si sottolinea che le violazioni della normativa a tutela dei diritti d'autore sul software impone la presenza nel sistema di software regolarmente licenziato, o comunque non protetto dal diritto d'autore. Comportamenti diversi sono sanzionati anche penalmente.
i) È obbligatorio rispettare le leggi in materia di sicurezza informatica. È vietato installare/utilizzare senza autorizzazione software che possa creare problemi di sicurezza o danneggiare la rete, come *port scanner, security scanner, network monitor, network flooder*, fabbriche di virus o di worm.
j) Salvo preventiva espressa autorizzazione del responsabile informatico 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 chiavette Internet, masterizzatori, modem, ecc.
k) I Notebook o Tablet in dotazione devono essere custoditi con diligenza, anche in relazione al rischio

di furti. In particolare è vietato lasciare tali strumenti incustoditi ed in vista all'interno di veicoli, dell'Ente o personali.

Si informa che i file creati con gli Strumenti e i relativi log, reperibili nella memoria degli Strumenti stessi, per ragioni tecniche rimangono registrati e possono essere oggetto di controllo da parte del Titolare del trattamento, attraverso Servizio IT consortile, per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio consortile.

I controlli possono avvenire secondo le disposizioni previste al successivo punto 5 del presente Regolamento.

Le informazioni così raccolte sono altresì utilizzabili a tutti i fini connessi al rapporto di lavoro, compresa la verifica del rispetto del presente Regolamento, che costituisce adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli ai sensi del Decreto Legislativo 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali".

3.2. Uso del File System consortile e degli Account Consortili

Il dipendente/collaboratore è consapevole che le risorse del File System (server, cartelle condivise, stampanti condivise, ecc.) e della rete Intranet del Consorzio di Bonifica Chiese e gli Account Consortili dei sistemi Operativi (Microsoft) sono necessari per rendere la prestazione lavorativa.

Ciascun dipendente / collaboratore si deve attenere alle seguenti regole di utilizzo del File System e della Rete Intranet.

a) Per garantire la sicurezza informatica e per motivi di organizzazione della produzione, l'Utente deve salvare ogni dato ed informazione sul Server aziendale, astenendosi dal salvataggio in locale (su desktop, sulla cartella "documenti" del proprio Strumento, ecc.).
b) È vietato il salvataggio sui server dell'Ente, ovvero sugli Strumenti, di documenti non inerenti l'attività lavorativa, quali a titolo esemplificativo documenti, fotografie, video, musica, pratiche personali, sms, mail personali, film e quant'altro. Ogni materiale personale rilevato dall'Amministratore di Sistema o responsabile informatico a seguito di interventi di sicurezza informatica ovvero di manutenzione/aggiornamento su server ed anche su Strumenti viene rimosso secondo le regole previste nel successivo punto 5 del presente Regolamento, ferma ogni ulteriore responsabilità civile, penale e disciplinare.
c) Senza il consenso del Titolare, è vietato trasferire documenti elettronici dai sistemi informativi e Strumenti dell'Ente a device esterni (hard disk, chiavette, CD, DVD e altri supporti).
d) Con regolare periodicità (almeno una volta al mese), ciascun utente provvede 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.
e) È vietato accedere alla rete aziendale con Strumenti personali, salvo l'utilizzo di reti o infrastrutture a ciò dedicate.
f) È vietato accedere alla rete Intranet con un codice d'identificazione utente diverso da quello assegnato. Le parole chiave d'ingresso alla rete ed ai programmi sono segrete e vanno comunicate e gestite secondo le procedure impartite.
g) I Sistemi Operativi degli Strumenti o degli applicativi (account Microsoft, ecc.) sono attivati dal

Servizio IT con Account consortili, che vengono gestiti dall'Ente e concessi in uso temporaneo all'Utente. E' vietato utilizzare gli Account ed i Servizi disponibili nel contesto degli Account (Repository, Cloud, Agenda, mail, Calendario, Note ecc.) per finalità personali.

h) Gli account dei Sistemi Operativi degli Strumenti o degli applicativi di smartphone e tablet Consortili (IOS, Android ecc.) anche se attivati personalmente dall'Utente e nella sua disponibilità, sono soggetti alle prescrizioni previste dal presente regolamento.

I log relativi all'uso del File System e della intranet consortile, nonché i file salvati o trattati su Server o sui router consortili quali strumenti elettronici dell'ente, sono registrati per la durata prevista dalla normativa vigente e possono essere oggetto di controllo da parte del Titolare del trattamento, attraverso il Servizio IT consortile, per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio consortile.

Si informa che gli Strumenti dell'Ente e/o i relativi Sistemi Operativi (IOS, Android ecc.) nonché gli altri Account necessari per il funzionamento degli Strumenti o degli applicativi (Microsoft ecc.) sono attivati dal Servizio IT con Account consortili e vengono gestiti dall'Ente e concessi in uso temporaneo all'Utente. La gestione dell'Account, ancorché concessa all'Utente, è effettuata dal Servizio IT che può accedere all'Account, vedendone il contenuto, per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio consortile. I dati contenuti negli Account Consortili verranno resettati alla riconsegna degli Strumenti ovvero alla cessazione dell'utilizzo del Servizio da parte dell'Utente.

Gli account dei Sistemi Operativi degli Strumenti o degli applicativi di smartphone e tablet Consortili (IOS, Android ecc.) attivati personalmente dall'Utente e nella Sua disponibilità, dovranno essere dallo stesso resettati alla cessazione dell'utilizzo del Servizio ovvero su richiesta del Servizio IT.

I controlli possono avvenire secondo le disposizioni previste al successivo punto 5 del presente Regolamento.

Le informazioni così raccolte sono altresì utilizzabili a tutti i fini connessi al rapporto di lavoro, compresa la verifica del rispetto del presente Regolamento, che costituisce adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli ai sensi del Decreto Legislativo 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali".

3.3. Uso dell'indirizzo di Posta elettronica

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

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

a) La casella di posta elettronica assegnata all'utente è di proprietà del Consorzio di Bonifica Chiese, ancorché sia strutturata riportando i dati anagrafici del dipendente/collaboratore. Essa è domicilio informatico dell'Ente ed è concessa esclusivamente quale strumento di lavoro.

b) È vietato utilizzare indirizzi di posta elettronica personali per finalità lavorative.

c) È vietato utilizzare la casella di posta elettronica aziendale quale user name / nome utente (ovvero come indirizzo mail di riferimento) per Servizi non inerenti l'attività lavorativa (es. per account di social network, servizi di e-commerce, registrazione a siti web, ecc.)

d) la partecipazione a catene telematiche o di Sant'Antonio. Se si dovessero peraltro ricevere messaggi di tale tipo, si deve comunicarlo immediatamente al personale del Servizio IT. Non si dovrà in alcun caso procedere all'apertura degli allegati a tali messaggi.

e) La casella di posta deve essere mantenuta in ordine, cancellando documenti inutili, obsoleti e soprattutto gli allegati ingombranti.

f) Ogni comunicazione inviata o ricevuta che abbia contenuti rilevanti o contenga impegni contrattuali o precontrattuali per il Consorzio di Bonifica Chiese ovvero contenga documenti da considerarsi riservati in quanto contraddistinti dalla dicitura "strettamente riservati" o da analoga dicitura, deve essere inoltrata all'Ufficio Protocollo.

g) È obbligatorio controllare con attenzione gli allegati di posta elettronica prima del loro utilizzo, verificando prima dell'apertura degli stessi ogni elemento che possa indurre a ritenere che si tratti di un VIRUS (es. se il mittente è sconosciuto, se il testo della mail presenti strani errori di battitura o un testo poco comprensibile ecc.). In caso di dubbio rivolgersi preventivamente al responsabile informatico.

h) È vietato effettuare l'apertura di file allegati alla posta elettronica che siano eseguibili (.exe), cartelle compresse (*.zip,.rar*, ecc.) soprattutto se provenienti da istituzioni bancarie o società di servizi (Enel, Eni, Wind, Telecom, Poste, ecc.)

i) Al fine di garantire la funzionalità del servizio di posta elettronica aziendale e di ridurre al minimo l'accesso ai dati, nel rispetto del principio di necessità e di proporzionalità, il sistema, in caso di assenze del dipendente/collaboratore (ad es. per ferie o attività di lavoro fuori sede dell'assegnatario della casella, o malattia) invierà automaticamente messaggi di risposta contenenti le "coordinate" di posta elettronica di un altro soggetto o altre utili modalità di contatto della struttura. In caso di assenze programmate la funzionalità deve essere attivata dall'utente; in caso di assenza non programmata (ad es. per malattia) verrà attivata a cura del responsabile informatico.

j) Al fine di ribadire agli interlocutori la natura esclusivamente aziendale della casella di posta elettronica, i messaggi devono contenere un avvertimento standardizzato nel quale sia dichiarata la natura non personale dei messaggi stessi precisando che, pertanto, il personale debitamente incaricato del Consorzio di Bonifica Chiese potrà accedere al contenuto del messaggio inviato alla stessa casella secondo le regole fissate nel presente regolamento.

Si informa che, ai sensi dell'articolo 2214 del Codice civile e dell'articolo 22 del Dpr 600/73, l'Ente conserva per dieci anni sui propri Server il contenuto di tutti i messaggi di posta elettronica con rilevanza giuridica e commerciale provenienti da e diretti a domini aziendali.

L'Ente, per il tramite del responsabile informatico, non controlla sistematicamente il flusso di comunicazioni mail né è dotato di sistemi per la lettura o analisi sistematica dei messaggi di posta elettronica ovvero dei relativi dati esteriori, al di là di quanto tecnicamente necessario per svolgere il servizio e-mail.

Tuttavia, in caso di assenza improvvisa o prolungata del dipendente ovvero per imprescindibili esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale ovvero per motivi di sicurezza del sistema informatico, l'Ente per il tramite del responsabile informatico può, secondo le procedure indicate successivo punto 5 del presente Regolamento, accedere all'account di posta elettronica aziendale, prendendo visione dei messaggi, salvando o cancellando file.

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

Le informazioni eventualmente raccolte sono altresì utilizzabili a tutti i fini connessi al rapporto di lavoro, compresa la verifica del rispetto del presente Regolamento, che costituisce adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli ai sensi del Decreto Legislativo 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali".

3.4. Uso della rete Internet e dei relativi servizi

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

a. Gli Strumenti assegnati al singolo utente possono essere abilitati alla navigazione in Internet. La rete Internet costituisce uno strumento aziendale utilizzabile esclusivamente per lo svolgimento della propria attività lavorativa.
b. Fermo quanto sopra, a titolo puramente esemplificativo, l'utente non potrà utilizzare la rete Internet per:
   - l'upload o il download di software, documenti, file multimediali (film, musica, ecc.) anche tramite software peer to peer;
   - l'effettuazione,durante l'orario di lavoro, di ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti on-line e simili, fatti salvi i casi direttamente autorizzati dal Legale Rappresentante o eventualmente dal Responsabile di Area / Funzione o dal Servizio IT e comunque nel rispetto delle normali procedure di acquisto;
   - la partecipazione a Forum e Social 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 Area / Funzione;
   - l'accesso, durante l'orario di lavoro, tramite internet, a siti non inerenti l'attività lavorativa nonché servizi web di qualsiasi genere non inerenti l'attività lavorativa (quali caselle webmail di posta elettronica personale, servizi online di Google / Apple / Microsoft ecc.).
c. Per motivi tecnici e di buon funzionamento del sistema informatico è buona norma, salvo comprovata necessità, non accedere a risorse web che impegnino in modo rilevante banda,

come a titolo esemplificativo: filmati (tratti da you tube, siti di informazione, siti di streaming ecc) o web radio, in quanto possono limitare e/o compromettere l'uso della rete agli altri utenti.

d. È vietato accedere ai social network (Facebook, Twitter, Linkedin, You Tube, Whatsapp, ecc) durante l'orario di lavoro. Il divieto si estende anche al caso di utilizzo di smartphone e tablet personali.

L'Ente, per il tramite del responsabile informatico, non effettua la memorizzazione sistematica delle pagine web visualizzate dal singolo Utente, né controlla con sistemi automatici i dati di navigazione dello stesso.

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

In tali casi i controlli avverranno nelle forme indicate al successivo punto 5 del presente Regolamento.

Le informazioni così raccolte sono altresì utilizzabili a tutti i fini connessi al rapporto di lavoro, compresa la verifica del rispetto del presente Regolamento, che costituisce adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli ai sensi del Decreto Legislativo 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali".

3.5. Telefonia cellulare, Smartphone e Tablet

Il dipendente è consapevole che il telefono, lo smartphone, il tablet assegnati nonché ogni applicazione in essi installata (di seguito anche Dispositivi) sono di proprietà del Consorzio di Bonifica Chiese e vengono affidati all'utente per rendere la prestazione lavorativa.

Pertanto ne viene concesso l'uso esclusivamente per lo svolgimento dell'attività lavorativa salva esplicita autorizzazione del Responsabile di Area.

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

a. L'eventuale uso promiscuo (anche per fini personali) di Dispositivi è possibile soltanto in presenza di preventiva autorizzazione scritta.
b. L'Utente è responsabile del corretto utilizzo e della custodia dei Dispositivi.

Si informa che il telefono, smartphone, tablet o dispositivo portatile vengono attivati con Account Consortili (vedi art. 3.2) concessi in uso temporaneo all'Utente.

Le informazioni relative all'utilizzo dei Dispositivi nonché i file con essi trattati (documenti, foto, video, messaggi ecc.), sono registrati nella memoria dei Dispositivi stessi ovvero possono lasciare traccia su Server e router aziendali, nelle relative bollette pervenute all'Ente ovvero nelle "aree personali" dei siti dei fornitori dei servizi di telefonia, ovvero sono trattati negli account di attivazione del dispositivo (es. microsoft, google, apple, etc.).

L'Ente non controlla sistematicamente tali informazioni, né sono installati software o sistemi in grado di monitore l'uso dei Dispositivi. Esclusivamente per inderogabili esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale, il responsabile informatico può

accedere a tali informazioni.

In caso di restituzione del Dispositivo, i dati saranno resettati.

I controlli possono avvenire secondo le disposizioni previste successivo punto 5 del presente Regolamento.

Le informazioni così raccolte sono altresì utilizzabili a tutti i fini connessi al rapporto di lavoro, compresa la verifica del rispetto del presente Regolamento, che costituisce adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli ai sensi del Decreto Legislativo 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali".

3.6. Multifunzione, Fax, Fotocopiatrici, Scanner, Plotter e altri strumenti (strumenti di stampa)

Il dipendente è consapevole che gli Strumenti di stampa sono di proprietà del Consorzio di Bonifica Chiese e sono affidati all'utente per rendere la prestazione lavorativa. Pertanto ne viene concesso l'uso esclusivamente per tale fine.

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

a. È vietato l'utilizzo delle multifunzioni, fotocopiatrici, scanner, plotter aziendali e altri strumenti di stampa per fini personali.
b. È necessario prestare attenzione alle fotocopie e alle stampe di documenti: copie mal riuscite, inutilizzate, minute, appunti ecc. devono essere eliminate utilizzando la macchina distruggi-documenti, ovvero sminuzzando i fogli in modo che risultino difficilmente leggibili.

3.7. Uso dei Dispositivi dotati del Sistema di Monitoraggio – GPS

Come da accordo sindacale e da "informativa completa di geolocalizzazione" che verrà fornita ai dipendenti, si informa che il Consorzio ha deciso di aumentare la sicurezza dei propri dipendenti che svolgono mansioni sul territorio tramite l'impiego di appositi apparecchi dotati di sistema di geolocalizzazione "Gps". Obiettivo del presente regolamento è normare l'utilizzo di tali apparecchiature evitando, tra l'altro, il loro danneggiamento.

Nell'utilizzare i **Dispositivi,** ciascun dipendente /collaboratore si dovrà attenere alle seguenti regole di utilizzo:

a. Non smontare gli apparecchi di geolocalizzazione: non rimuovere la copertura o le viti, così da evitare sbalzi elettrici. All'interno non ci sono parti riutilizzabili. In caso di necessità, rivolgersi a personale qualificato indicato dal Consorzio;
b. Non tentare di disabilitare o intervenire in qualsiasi modo sugli apparecchi di geolocalizzazione. Ogni intervento manutentivo verrà effettuato da personale specializzato debitamente incaricato dal Consorzio;
c. È vietata la manomissione delle antenne delle apparecchiature GPS e l'utilizzo di strumenti hardware/software in grado di interferire sulla ricezione e trasmissione del segnale;
d. Conservarli e maneggiarli con cura: tali Dispositivi possono danneggiarsi se utilizzati o conservati in modo improprio;
e. Non lasciarli in ambienti particolarmente caldi (ad esempio nell'automobile, esposto direttamente alla luce solare). Temperature troppo elevate possono ridurre la durata dei circuiti elettronici, danneggiare le batterie e deformare o fondere le parti in plastica;
f. Non lasciarli in ambienti particolarmente freddi: è infatti possibile la formazione di

condensa che può danneggiare i circuiti elettronici;

g. Durante lo svolgimento della propria prestazione lavorativa, anche per le finalità specificate in modo più dettagliato nel riquadro sottostante, avere cura di portarli sempre con sé;
h. Evitare di consegnare a colleghi e/o soggetti terzi il Dispositivo ricevuto.

L'utilizzatore in caso di guasto, provocato o subito, del Dispositivo a lui affidato, informerà immediatamente dell'accaduto il proprio Responsabile di Area / Funzione. L'Ente si riserva di effettuare tutti gli opportuni controlli sul corretto utilizzo dell'apparecchiatura, nel rispetto comunque delle normative vigenti.

Si rende altresì noto che i trattamenti di dati personali effettuati dall'Ente mediante il sistema di localizzazione GPS, avverrà correttamente, lecitamente, e conformemente a quanto previsto dalla disciplina rilevante in materia di sicurezza e protezione dei dati personali.

I Dispositivi dotati del Sistema di Monitoraggio – GPS saranno forniti al dipendente/collaboratore per rendere la prestazione lavorativa; non è possibile tramite essi risalire, in tempo reale, al luogo dove si trova il personale dipendente. Se indossati correttamente, solamente per le finalità sotto descritte, tali Dispositivi trasmettono tramite sms, le proprie coordinate GPS ad un responsabile del Consorzio affinchè egli possa intraprendere le misure ritenute necessarie. Non è prevista raccolta o registrazione dei dati di geolocalizzazione.

Si informa che i dati ottenuti per le finalità sopra descritte saranno altresì utilizzabili a tutti i fini connessi al rapporto di lavoro, visto che la presente informativa ed il Regolamento sull'uso degli strumenti aziendali costituiscono adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli, sempre nel rispetto di quanto disposto dal Decreto Legislativo 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali".

FINALITA'	**SPECIFICAZIONE FINALITA'**	**DURATA CONSERVAZIONE DATI**
1) Sicurezza dei lavoratori e dei luoghi di lavoro	migliorare la sicurezza dei lavoratori fuori sede ed in situazioni di isolamento, anche in ossequio alle disposizioni del D.lgs 81/08, con la fornitura di DISPOSITIVI dotati di sensori c.d. "uomo a terra" in grado di individuare movimenti innaturali o posture a rischio, tasti di chiamata di emergenza ecc., che associati alla geolocalizzazione consentirà all'Ente verifiche di eventuali situazioni di emergenza e l'invio tempestivo di soccorsi;	Non è prevista conservazione dei dati

Le disposizioni di cui sopra diverranno efficaci nel momento in cui verranno i dispositivi verranno consegnati ai dipendenti.

4. Gestione delle credenziali di autenticazione agli strumenti e servizi aziendali

4.1. Principi generali

Il rilascio, la modifica o la cancellazione di credenziali di autenticazione che permettono l'accesso a Strumenti, posta elettronica, rete, Server dell'Ente, ecc. vengono effettuati dal responsabile informatico, previa espressa indicazione del Capo Area o Capo Settore.

Le credenziali di autenticazione consistono in un codice per l'identificazione dell'utente (user id), assegnato dal responsabile informatico, associato ad una parola chiave (password) riservata che deve essere custodita dall'incaricato con la massima diligenza.

È vietato comunicare a soggetti terzi le proprie credenziali.

Se necessario far accedere terzi ai sistemi informativi protetti da una propria password, si prega di rivolgersi al responsabile informatico.

È fatto assoluto divieto di trascrivere la parola chiave nei pressi della postazione di lavoro.

La parola chiave, 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 all'incaricato.

È necessario prestare particolare attenzione a non essere osservati mentre si digita la password o qualunque codice di accesso ai sistemi informatici. Infatti, anche se molti programmi non ripetono in chiaro la password sullo schermo, l'attenta osservazione da parte altrui dei tasti digitati può condurre all'individuazione della parola chiave.

È necessario procedere alla modifica della parola chiave a cura dell'utente, incaricato del trattamento, al primo utilizzo e, successivamente, almeno ogni tre mesi. Si informa che il sistema assegna di default un termine di validità delle password: qualora l'utente non provveda a variare la propria password in tempo, l'accesso al personal computer e/o al sistema verrà temporaneamente bloccato.

Qualora la parola chiave dovesse venir sostituita in quanto abbia perso la propria riservatezza, si procederà a sostituirla come da modalità descritta nel presente Regolamento d'intesa con il personale dell'Ufficio IT.

Le credenziali di accesso rilasciate non sono conosciute dagli Amministratori di Sistema.

5. Controlli sugli strumenti (art. 6.1 Provv. Garante, ad integrazione dell'informativa ex art. 13 d.lgs 196/03)

5.1. Principi generali

L'uso degli Strumenti Informatici dell'Ente può lasciare traccia delle informazioni sul relativo uso, come analiticamente spiegato nei riquadri di cui ai punti 3.1 – 3.2. – 3.3 – 3.4 – 3.5 e 3.7 del presente Regolamento.

Tali informazioni, che possono contenere dati personali eventualmente anche sensibili dell'Utente, possono essere oggetto di controlli da parte dell'Ente, per il tramite dell'Amministratore di Sistema, volti a garantire esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale, nonché per la sicurezza e la salvaguardia del sistema informatico, per ulteriori motivi tecnici e/o manutentivi (ad es. aggiornamento / sostituzione / implementazione di programmi, manutenzione hardware, etc.).

Tali interventi di controllo (di seguito descritti) possono permettere all'Ente di prendere indirettamente cognizione dell'attività svolta con gli strumenti.

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

Qualora risulti necessario l'accesso alle risorse informatiche e relative informazioni descritte ai punti 3.1 – 3.2. – 3.3 – 3.4 – 3.5 il Responsabile del trattamento dei dati personali per il tramite del responsabile informatico, si atterrà al processo descritto qui di seguito (se e in quanto compatibile con lo Strumento oggetto di controllo).

1. Avviso generico a tutti i dipendenti della presenza di comportamenti anomali che possono mettere a rischio la sicurezza del sistema informativo e richiamo all'esigenza di attenersi al rispetto del presente Regolamento.
2. Successivamente, dopo almeno 7 giorni, se il comportamento anomalo persiste, l'Ente potrà autorizzare il personale addetto al controllo, potendo così accedere alle informazioni descritte ai punti 3.1 – 3.2. – 3.3 – 3.4 – 3.5, con possibilità di rilevare files trattati, siti web visitati, software installati, documenti scaricati, statistiche sull'uso di risorse ecc. nel corso dell'attività lavorativa. Tale attività potrà essere effettuata in forma anonima ovvero tramite controllo del numero IP, dell'Utente e con l'identificazione del soggetto che non si attiene alle istruzioni impartite.

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

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

Qualora indirettamente si riscontrino file o informazioni anche personali, esse potranno essere altresì utilizzabili a tutti i fini connessi al rapporto di lavoro, considerato che il presente Regolamento costituisce adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli, sempre nel rispetto di quanto disposto dal Decreto Legislativo 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali".

5.3. Controlli per esigenze produttive e di organizzazione

Per esigenze produttive e di organizzazione si intendono – fra le altre – l'urgente ed improrogabile

necessità di accedere a files o informazioni lavorative di cui si è ragionevolmente certi che siano disponibili su risorse informatiche di un Utente (quali file salvati, posta elettronica, SMS ecc) che non sia reperibile, in quanto ad esempio assente, temporaneamente irreperibile ovvero cessato.

Qualora risulti necessario l'accesso alle risorse informatiche e relative informazioni descritte ai punti 3.1 – 3.2. – 3.3 – 3.4 – 3.5 e 3.7 il Responsabile del trattamento dei dati personali, per il tramite del responsabile informatico, si atterrà alla procedura descritta qui di seguito (se e in quanto compatibile con lo Strumento oggetto di controllo).

1. Redazione di un atto da parte del Direttore e/o Capo Area che comprovi le necessità produttive e di organizzazione che richiedano l'accesso allo Strumento.
2. Incarico all'Amministratore di sistema di accedere alla risorsa con credenziali di Amministratore ovvero tramite l'azzeramento e la contestuale creazione di nuove credenziali di autenticazione dell'Utente interessato, con avviso che al primo accesso alla risorsa, lo stesso dovrà inserire nuove credenziali.
3. Redazione di un verbale che riassuma i passaggi precedenti.
4. In ogni caso l'accesso ai documenti presenti nella risorsa è limitato a quanto strettamente indispensabile alle finalità produttive e di organizzazione del lavoro.
5. Qualora indirettamente si riscontrino file o informazioni anche personali, esse potranno essere altresì utilizzabili a tutti i fini connessi al rapporto di lavoro, considerato che il presente Regolamento costituisce adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli, sempre nel rispetto di quanto disposto dal Decreto Legislativo 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali".

6. Partecipazioni a social media

6.1. L'utilizzo a fini promozionali e commerciali di Facebook, Twitter, Linkedin, dei blog e dei forum, anche professionali (ed altri siti o social media) è gestito ed organizzato esclusivamente 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.

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

6.3. Il presente articolo deve essere osservato dall'Utente sia che utilizzi dispositivi messi a disposizione dall'Ente, sia che utilizzi propri dispositivi, sia che partecipi ai social media a titolo personale, sia che lo faccia per finalità professionali, come dipendente dell'Ente.

6.4. La condivisione dei contenuti nei social media deve sempre rispettare e garantire la segretezza sulle informazioni aziendali considerate dall'Ente riservate ed in genere, a titolo esemplificativo e non esaustivo, sulle informazioni inerenti attività, progetti, procedimenti svolti o in svolgimento presso gli uffici. Inoltre, ogni comunicazione e divulgazione di contenuti dovrà essere effettuata nel pieno rispetto dei diritti di proprietà industriale e dei diritti d'autore, sia di terzi che dell'Ente.L'utente, nelle proprie comunicazioni, non potrà quindi inserire il nominativo e il logo dell'Ente, né potrà pubblicare disegni, modelli od altro connesso ai citati diritti. Ogni deroga a quanto sopra disposto potrà peraltro avvenire solo previa specifica autorizzazione della Direzione.

6.5. L'utente deve garantire la tutela della riservatezza e dignità delle persone; di conseguenza, non potrà comunicare o diffondere dati personali (quali dati anagrafici, immagini, video, suoni e voci) di colleghi e in genere di collaboratori aziendali, se non con il preventivo personale consenso di questi, e comunque non potrà postare nel social media immagini, video, suoni e voci registrati all'interno dei luoghi di lavoro aziendali, se non con il preventivo consenso del Responsabile d'ufficio.

6.6. Qualora l'utente intenda usare social network, blog, forum su questioni anche indirettamente professionali (es. post su prodotti, servizi, fornitori, partner, ecc.) egli esprimerà unicamente le proprie opinioni personali; pertanto, ove necessario od opportuno per la possibile connessione con l'Ente, in particolare in forum professionali, l'utente dovrà precisare che le opinioni espresse sono esclusivamente personali e non riconducibili all'Ente.

7. Sanzioni

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

Eventuali violazioni del presente Regolamento da parte dei dipendenti nonché di altre norme previste dal CCNL applicato, a seconda della gravità della infrazione, comportano l'adozione dei seguenti provvedimenti:

- censura scritta;
- sospensione dal servizio;
- licenziamento in tronco;
- licenziamento di diritto.

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

È richiamato in questa sede il codice disciplinare, affisso in bacheca ed accessibile a tutto il personale dipendente.

8. Aggiornamento e revisione

8.1 Il presente Regolamento è soggetto a revisione con frequenza annuale da parte dell Responsabile del Trattamento.