ORDINE DEI PERITI INDUSTRIALI
E DEI PERITI INDUSTRIALI LAUREATI
della Provincia di Vicenza

Regolamento per l'utilizzo dei sistemi e strumenti informatici

Firmato
Il Presidente
Gasparotto Per. Ind. Manuel

Consiglio Direttivo 2018-2022

Gasparotto Per. Ind. Manuel	Presidente	
Sofia Per. Ind. Antonio	Tesoriere	
Caldarde Per. Ind. Mauro	Segretario	
Conte Per. Ind Damiano	Consigliere	
Corato Per. Ind. Giovanni	Consigliere	
Crivellaro Per. Ind. Martino	Consigliere	
Marchetti Per. Ind. Susanna	Consigliere	
Scambi Per. Ind. Pierdavide	Consigliere	

Revisioni regolamento

Rev.	Data	Motivo	Redatto	Verificato	Approvato
00	01/2020	Prima emissione	E.E.	G.M.	Consiglio ODG 633 17/02/2020
01	08/11/2021	Modifica gestione password	G.M.	G.M.	Delibera n. 192/2021 ODG 665

1 INDICE

2 Entrata in vigore del Regolamento

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

2.2 Copia del Regolamento, oltre ad essere affisso nella bacheca dell'Ordine dei Periti Industriale e dei Periti Industriali Laureati della Provincia di Vicenza (da qui in avanti identificato con la parola "Ordine") anche per quanto prevede l'art.7 della Legge n. 300/1970 e successive modifiche ed integrazioni verrà consegnato a ciascun dipendente, oltre che a collaboratori, consulenti od altri incaricati esterni (es. incaricati software house, professionisti di cui si avvale, etc.) che venissero autorizzati a far uso di strumenti informatici o ad accedere alla rete informatica e ad eventuali dati ed informazioni ivi conservati e trattati.

3 Campo di applicazione del Regolamento

3.1 Il nuovo Regolamento si applica a tutti i dipendenti, senza distinzione di ruolo e/o livello, nonché a tutti i collaboratori e consulenti a prescindere dal rapporto contrattuale intrattenuto che venissero autorizzati a far uso di strumenti tecnologici o di accedere alla rete informatica e ad eventuali dati ed informazioni ivi conservati e trattati. Pertanto, le regole di seguito previste devono intendersi a carico tanto dei primi quanto dei secondi, ferma restando la necessità che si dia opportuno conto del presente Regolamento nel contratto concluso con quest'ultimi.

3.2 Ai fini delle disposizioni dettate per l'utilizzo delle risorse informatiche, per "utente" deve così intendersi ogni dipendente, collaboratore e/o consulente in possesso di specifiche credenziali di autenticazione. Tale figura potrà anche venir indicata quale "responsabile esterno del trattamento" od "incaricato del trattamento", in ragione delle attività e degli impegni che si assume nell'organizzazione od a favore dell'Ordine stessa.

4 Utilizzo del Personal Computer

4.1 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 da parte degli assegnatari evitando ogni possibile forma di danneggiamento.

4.2 Il personal computer dato in affidamento all'utente permette l'accesso alla rete solo attraverso specifiche credenziali di autenticazione come meglio descritto al successivo punto 4 del presente Regolamento.

4.3 L'Ordine rende noto che il Responsabile Trattamento Dati o suo Delegato è stato 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. La stessa facoltà, sempre ai fini della sicurezza del sistema e per garantire la normale operatività, si applica anche in caso di assenza prolungata o impedimento dell'utente. Qualora lo specifico intervento dovesse comportare anche l'accesso a contenuti delle singole postazioni PC, il personale incaricato ne darà comunicazione agli utenti interessati, preventivamente ovvero, nel caso di urgenza dell'intervento stesso, successivamente ad esso.

4.4 Il Responsabile Trattamento Dati o suo delegato ha la facoltà di collegarsi e visualizzare in remoto i contenuti delle singole postazioni PC al fine di garantire l'assistenza tecnica e la normale attività operativa nonché la massima sicurezza contro virus, spyware, malware, etc. 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, e sempre che non si pregiudichi la necessaria tempestività ed efficacia dell'intervento, verrà data comunicazione della necessità dell'intervento stesso.

4.5 Non è consentito l'uso di programmi diversi da quelli ufficialmente installati dal personale incaricato 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 l'Ordine a gravi responsabilità civili; si evidenzia, inoltre, 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, vengono sanzionate penalmente e possono anche comportare il sorgere di una responsabilità amministrativa a carico dell'Ordine, come disposta dall'art. 25-nonies del D.lgs. 8 giugno 2001, n. 231, con applicazione di sanzioni pecuniarie ed interdittive.

4.6 Salvo preventiva espressa autorizzazione del personale incaricato, 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 USB, …).

4.7 Ogni utente deve prestare la massima attenzione ai supporti di origine esterna, avvertendo immediatamente il personale incaricato nel caso in cui siano rilevati virus e adottando quanto previsto dal successivo punto 10 del presente Regolamento relativo alle procedure di protezione antivirus.

4.8 Il Personal Computer deve essere spento ogni sera prima di lasciare gli uffici e quando incustodito, bloccato con un salva-schermo e protetto con password. Lasciare un elaboratore incustodito sbloccato 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.

5 Gestione e assegnazione delle credenziali di autenticazione

5.1 Le credenziali di autenticazione per l'accesso alla rete vengono assegnate dal personale incaricato, previa espressa indicazione del Responsabile Trattamento Dati o suo Delegato.

5.2 Le credenziali di autenticazione consistono in un codice per l'identificazione dell'utente (user id), assegnato dal personale incaricato, associato ad una parola chiave (password) riservata che dovrà venir custodita dall'incaricato con la massima diligenza e non divulgata. Non è consentita l'attivazione della password di accensione (bios), senza preventiva autorizzazione da parte del personale incaricato.

5.3 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.

5.4 È necessario procedere alla modifica della parola chiave a cura dell'utente, incaricato del trattamento, al primo utilizzo e, successivamente, almeno ogni sei mesi o al verificarsi di eventi che ne determinano la perdita di riservatezza.

5.5 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 Responsabile Trattamento Dati o suo Delegato.

5.6 Soggetto preposto alla custodia delle credenziali di autenticazione è il Responsabile Trattamento dati.

Gestione credenziali di accesso a software o servizi online

5.7 Per l'accesso a software/applicazioni/piattaforme per l'utilizzo di servizi e applicativi sia online che offline si prevede un aggiornamento con cadenza almeno annuale delle password/credenziali, salvo eventuali diverse disposizioni valutate e definite puntualmente dal Responsabile Trattamento dati.

5.8 Comunicazione di eventuali variazioni alle credenziali o di attivazione di nuovi account dovranno essere fornite al Responsabile Trattamento dati, secondo Sue disposizioni e modalità, dando indicazione anche dei nominativi con cui è stato eventualmente condiviso il dato (es: fornitore assistenza software/applicativi, Responsabile servizi Informatici, ecc..).

5.9 Ove possibile, si procederà ad avere almeno due credenziali di accesso per servizi e applicativi in uso all'Ordine.

5.10 Qualora l'accesso tramite credenziali ad uno dei servizi o applicativi sopra citati sia consentito ad un solo utente, le stesse credenziali verranno condivise con il Responsabile Trattamento dati al fine di permettere una continuità operativa in caso di assenza prolungata o impedimento dell'utente ad accedere al servizio.

6 UTILIZZO DELLA RETE

6.1 Per l'accesso alla rete ciascun utente deve utilizzare la propria credenziale di autenticazione.
È assolutamente proibito entrare nella rete e nei programmi 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.

6.2 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. Su queste unità vengono svolte regolari attività di manutenzione, amministrazione e back up da parte del personale incaricato.

6.3 Il personale incaricato può in qualunque momento procedere alla rimozione di ogni file o applicazione che riterrà essere pericolosi per la Sicurezza sia sui PC degli incaricati sia sulle unità di rete.

6.4 Risulta opportuno che, con regolare periodicità (almeno ogni sei 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.

6.5 Nella gestione dei sistemi informatici, il personale incaricato potrà acquisire informazioni generate dalle funzionalità insite negli stessi sistemi, quali, ad esempio, le informazioni sugli orari di accensione e spegnimento dei personal computer, rilevati automaticamente tramite il sistema di autenticazione al dominio di rete, e i log degli accessi a specifiche risorse di rete (file o cartelle). Tali informazioni potranno essere utilizzate, ai sensi del successivo punto 12.2, per tutti i fini connessi al rapporto di lavoro, sempre nell'ambito delle finalità individuate nel precedente punto 3, e con espressa esclusione di qualsiasi forma di controllo sistematico e costante nei confronti degli utenti degli stessi sistemi.

7 UTILIZZO DI ALTRI DISPOSITIVI ELETTRONICI

7.1 Tutti i dispositivi elettronici dati in dotazione al personale devono considerarsi strumenti di lavoro: ne viene concesso l'uso esclusivamente per lo svolgimento delle attività lavorative, non essendo quindi consentiti utilizzi a carattere personale o comunque non strettamente inerenti le attività lavorative. Fra i dispositivi in questione vanno annoverati eventuali telefoni, PC portatili, tablet, telefoni cellulari, etc., indipendentemente dal fatto che l'utente abbia o meno la possibilità di accedere alla rete o di condividere documenti, dati e materiali ivi conservati e/o trattati.

7.2 L'utente resta responsabile del singolo dispositivo assegnato e deve custodirlo con diligenza sia durante trasferte e spostamenti sia durante l'utilizzo nel luogo di lavoro; va sempre adottata ogni cautela per evitare danni o sottrazioni.

7.3 I dispositivi vanno protetti adeguatamente attivando un codice di blocco (codice PIN , password , faceID, fingerprint, etc.); va mantenuto aggiornato il software di base del dispositivo e le applicazioni installate; servizi di connettività wifi, NFC e bluetooth vanno disattivate quando non utilizzate.

7.4 Con riferimento ai telefoni cellulari, 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 SMS o MMS di natura personale o comunque non pertinenti rispetto allo svolgimento dell'attività lavorativa, viene consentita solo nel caso di comprovata necessità ed urgenza. Inoltre, l'eventuale uso promiscuo (anche per fini personali) del telefono cellulare è possibile soltanto in presenza di preventiva autorizzazione scritta e in conformità delle istruzioni al riguardo impartite dal personale incaricato.

7.5 Si precisa, peraltro, che le disposizioni previste nel presente Regolamento ai punti 3, 7, 8, 9, 10 e 11 dello stesso trovano applicazione anche nell'uso dei dispositivi elettronici qui considerati.

7.6 Viene infine disposto il divieto di utilizzo per fini personali di fax, per spedire o per ricevere documentazione, e/o di fotocopiarli, salva diversa esplicita autorizzazione da parte del Responsabile Trattamento Dati.

8 UTILIZZO E CONSERVAZIONE DEI SUPPORTI RIMOVIBILI

8.1 Tutti i supporti magnetici rimovibili (CD e DVD riscrivibili, supporti USB, ecc.), contenenti dati sensibili nonché informazioni costituenti know-how o database contenenti dati personali o personali con caratteristiche particolari, devono essere trattati con particolare cautela onde evitare che il loro contenuto possa essere trafugato o alterato e/o distrutto o, successivamente alla cancellazione, recuperato.

8.2 L'utente resta, in ogni caso responsabile della custodia dei supporti e dei dati in essi contenuti; in particolare, i supporti magnetici contenenti dati sensibili devono essere dagli utenti adeguatamente custoditi in armadi chiusi.

8.3 Viene severamente vietato l'utilizzo di supporti rimovibili personali.

8.4 Al fine di assicurare la distruzione e/o inutilizzabilità di supporti magnetici rimovibili contenenti dati particolari, ciascun utente dovrà contattare il personale incaricato e seguire le istruzioni da questo impartite. Nel caso di dispositivi elettronici, con riferimento in particolare a PC portatili, tablet ed altri dispositivi sui quali possano venir salvati documenti, dati ed altro materiale, dovrà farsi particolare attenzione al salvataggio in opportuni supporti esterni di tale materiale oppure alla sua rimozione effettiva prima della riconsegna del dispositivo, concordata comunque ogni opportuna azione al riguardo con il personale incaricato.

9 USO DELLA POSTA ELETTRONICA

9.1 La casella di posta elettronica assegnata all'utente è uno strumento di lavoro. Le persone assegnatarie delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse.

9.2 È fatto divieto di utilizzare le caselle di posta elettronica **nomecognome@XXXX.it** per motivi diversi da quelli strettamente legati all'attività lavorativa. In questo senso, a titolo puramente esemplificativo, l'utente non potrà utilizzare la posta elettronica per:

a) l'invio e/o il ricevimento di allegati contenenti filmati o brani musicali (es. mp3) non legati all'attività a) lavorativa;

b) l'invio e/o il ricevimento di messaggi personali o per la partecipazione a dibattiti, aste on line, concorsi, forum o mailing-list;

c) la partecipazione a catene telematiche. Se si dovessero peraltro ricevere messaggi di tale tipo, si deve comunicarlo immediatamente al personale incaricato. Non si dovrà in alcun caso procedere all'apertura degli allegati a tali messaggi.

9.3 La casella di posta deve essere mantenuta in ordine, cancellando documenti inutili o non costituenti corrispondenza commerciale e soprattutto allegati ingombranti. In caso di cessazione del rapporto di lavoro, il singolo dipendente è tenuto ad eliminare dalle proprie cartelle tutti i messaggi di posta elettronica ed i documenti non pertinenti l'attività svolta e non utili alle esigenze, mantenendo integra, invece, tutta la corrispondenza e documentazione inerente alla attività lavorativa. Resta inteso che, di conseguenza, la documentazione presente nel profilo del singolo utente che cessa il rapporto di lavoro verrà considerata presuntivamente quale corrispondenza e documentazione lavorativa e non personale.

9.4 Ogni comunicazione inviata o ricevuta che abbia contenuti rilevanti o contenga impegni contrattuali o precontrattuali ovvero contenga documenti da considerarsi riservati in quanto contraddistinti dalla dicitura "strettamente riservati" o da analoga dicitura, deve essere visionata od autorizzata dal Responsabile Trattamento Dati.

9.5 Poiché la casella di posta assegnata costituisce strumento di lavoro, è opportuno evidenziare che i messaggi ivi contenuti, avendo presuntivamente natura di corrispondenza commerciale, verranno conservati nei server per 10 anni, a norma dell'art. 2220 del Codice civile.

9.6 È possibile utilizzare la ricevuta di ritorno per avere la conferma dell'avvenuta lettura del messaggio da parte del destinatario.

9.7 È obbligatorio porre la massima attenzione nell'aprire i file attachments di posta elettronica prima del loro utilizzo (non eseguire download di file eseguibili o documenti da siti Web o Ftp non conosciuti).

9.8 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, il sistema, in caso di assenze programmate (ad es. per ferie o attività di lavoro fuori sede dell'assegnatario della casella) invierà automaticamente messaggi di risposta contenenti le coordinate di posta elettronica di un altro soggetto o altre utili modalità di contatto. In tal caso, la funzionalità deve essere attivata e disattivata dall'utente.

9.9 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 del Responsabile Trattamento Dati o suo Delegato.

9.10 Sarà comunque consentito al superiore gerarchico dell'utente o, comunque, sentito l'utente, a persona individuata dall'Ordine, accedere alla casella di posta elettronica dell'utente per ogni ipotesi in cui si renda necessario (ad es.: mancata attivazione della funzionalità di cui al punto 9.7; assenza non programmata ed impossibilità di attendere i due giorni di cui al punto 9.8).

9.11 Il personale incaricato, nell'impossibilità di procedere come sopra indicato e nella necessità di non pregiudicare la necessaria tempestività ed efficacia dell'intervento, potrà accedere alla casella di posta elettronica per le sole finalità indicate al punto 3.3.

9.12 Al fine di ribadire agli interlocutori la natura esclusivamente dell'Ordine 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 potrà accedere al contenuto del messaggio inviato alla stessa casella secondo le regole fissate nella propria policy.

9.13 L'Ordine si riserva la facoltà, a proprio insindacabile giudizio, di assegnare o ritirare l'utilizzo della casella di posta elettronica in base alla propria esclusiva e insindacabile valutazione della necessità di utilizzo della stessa per lo svolgimento delle attività lavorative.

9.14 La casella di posta elettronica, unitamente alle credenziali di autenticazione per l'accesso alla rete, viene disattivata al momento della conclusione del rapporto di lavoro che ne giustificava l'assegnazione. L'Ordine si riserva, tuttavia, di valutare a proprio esclusivo ed insindacabile giudizio la necessità di mantenere attiva in ricezione la casella per un congruo periodo di tempo al fine di garantire la funzionalità; in tal caso:

- avranno accesso alla casella esclusivamente dipendenti incaricati in funzione alle mansioni lavorative assegnate;
- verranno inviate mail ai mittenti con indicazione della diversa casella di posta elettronica cui trasmettere i messaggi;
- viene escluso, comunque, l'invio di messaggi da tale casella di posta.

9.15 Nel caso in cui venisse assegnato all'utente anche la gestione di uno o più indirizzi di posta elettronica certificata di cui l'Ordine si fosse dotata, tale utente dovrà attenersi alle regole previste in questo Regolamento.

10 NAVIGAZIONE IN INTERNET

10.1 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.

10.2 In questo senso, a titolo puramente esemplificativo, **l'utente non potrà utilizzare internet** per:

- l'upload o il download di software anche gratuiti (freeware o shareware), nonché l'utilizzo di documenti provenienti da siti web se non strettamente attinenti all'attività lavorativa (filmati e musica) e previa verifica dell'attendibilità dei siti in questione (nel caso di dubbio, dovrà venir a tal fine contattato il personale incaricato);
- l'effettuazione 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 Responsabile Trattamento dati 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'iscrizione con account e la partecipazione personale a social network, l'utilizzo di chat line (esclusi gli strumenti autorizzati), di bacheche elettroniche e le registrazioni in guest books anche utilizzando pseudonimi (o nicknames) se non espressamente autorizzati dal Responsabile d'ufficio;
- l'accesso, tramite internet, a caselle webmail di posta elettronica personale.

10.3 Al fine di evitare la navigazione in siti non pertinenti all'attività lavorativa, l'Ordine rende peraltro nota l'adozione di uno specifico sistema di blocco o filtro automatico che prevengano determinate operazioni quali l'upload o l'accesso a determinati siti inseriti in una "black list".

10.4 Gli eventuali controlli, compiuti dal personale incaricato ai sensi del precedente punto 10.3, potranno avvenire mediante un sistema di controllo dei contenuti (Proxy server) o mediante "file di log" della navigazione svolta. Il controllo sui file di log non è continuativo ed i file stessi vengono conservati non oltre 12 mesi, ossia il tempo indispensabile per il corretto perseguimento delle finalità organizzative e di sicurezza dell'Ordine.

10.5 L'utilizzo di tutte le reti WiFi presenti nell'Ordine è limitato agli utenti autorizzati. A tale scopo si precisa che l'utilizzo di qualsiasi rete WiFi disponibile nell'Ordine e dalla stessa configurata è possibile solo a seguito di digitazione di specifiche credenziali che vengono assegnate dal personale incaricato.

10.6 L'accesso da remoto alla rete dell'Ordine è possibile agli utenti abilitati solo a seguito di comunicazione di specifiche credenziali o dell'installazione di software che lo abilita sui dispositivi in uso.
L'accesso da remoto alla rete è possibile solo utilizzando i dispositivi previsti. A tale scopo vengono svolti controlli automatici che impediscono l'accesso utilizzando dispositivi non abilitati.

11 PROTEZIONE ANTIVIRUS

11.1 Il sistema informatico è protetto da software antivirus aggiornato periodicamente. Ogni utente deve comunque tenere comportamenti tali da ridurre il rischio di attacco al sistema informatico mediante virus o mediante ogni altro software aggressivo.

11.2 Nel caso il software antivirus rilevi la presenza di un virus, l'utente dovrà immediatamente sospendere ogni elaborazione in corso senza spegnere il computer nonché segnalare prontamente l'accaduto al Responsabile trattamento Dati o suo Delegato.

11.3 Ogni dispositivo di provenienza esterna dovrà essere verificato mediante il programma antivirus prima del suo utilizzo e, nel caso venga rilevato un virus, dovrà essere prontamente consegnato al Responsabile Trattamento Dati o suo Delegato.

12 PARTECIPAZIONI A SOCIAL MEDIA

12.1 L'utilizzo a fini promozionali e commerciali dei social media – quali ad esempio Facebook™, Twitter™, Linkedin™, dei blog e dei forum, anche professionali – verrà gestito ed organizzato esclusivamente attraverso specifiche direttive ed istruzioni operative al personale a ciò espressamente addetto, rimanendo

escluse iniziative individuali da parte dei singoli utenti (conformemente a quanto disposto al precedente punto 10.2).

12.2 Fermo restando il pieno ed inderogabile diritto della persona alla libertà di espressione ed al libero scambio di idee ed opinioni, l'Ordine ritiene comunque opportuno indicare agli utenti alcune regole comportamentali, al fine di tutelare tanto la propria immagine, 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 viene vietata la partecipazione agli stessi social media durante l'orario di lavoro. La policy qui dettata deve venir seguita dagli utenti sia che utilizzino dispositivi messi a disposizione, sia che utilizzino propri dispositivi, sia che partecipino ai social media a titolo personale, sia che lo facciano per finalità professionali, come dipendenti.

12.3 La condivisione dei contenuti nei social media deve sempre rispettare e garantire la segretezza sulle informazioni considerate riservate ed in genere, a titolo esemplificativo e non esaustivo, sulle informazioni finanziarie ed economiche, commerciali, sugli iscritti, sui fornitori ed altri partners. 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'Ordine; l'utente, nelle proprie comunicazioni, non potrà quindi inserire marchi od altri segni distintivi del collegio, né potrà pubblicare disegni, modelli od altro connesso ai citati diritti. Ogni deroga a quanto sopra disposto potrà peraltro avvenire solo previa specifica autorizzazione dal Responsabile Trattamento dati.

12.4 L'utente deve garantire la tutela della privacy 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, 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, se non con il preventivo consenso del Responsabile d'ufficio.

12.5 L'utente risponde personalmente dei propri comportamenti e deve astenersi dal porre in essere, nei confronti in genere di terzi e specificatamente verso l'Ordine, i colleghi, i clienti ed i fornitori, attività che possano essere penalmente o civilmente rilevanti; a titolo esemplificativo, sono quindi vietati comportamenti ingiuriosi, diffamatori e denigratori, discriminatori o che configurano molestie. In tal senso, è vivamente auspicato da parte di tutti un comportamento civile e sobrio, in particolar modo in qualunque occasione in cui l'espressione o il contesto in cui essa avviene possa essere collegata all'ambito dell'Ordine.

12.6 Infine, in via generale ed ove non autorizzato in senso diverso dal proprio Responsabile Trattamento Dati, l'utente, nell'uso dei social network, esprimerà unicamente le proprie opinioni personali; pertanto, ove necessario od opportuno per la possibile connessione con l'Ordine, in particolare in forum professionali, l'utente dovrà precisare che le opinioni espresse sono esclusivamente personali e non riconducibili all'Ordine.

13 OSSERVANZA DELLE DISPOSIZIONI IN MATERIA DI PRIVACY

13.1 È obbligatorio attenersi alle disposizioni in materia di Privacy e di misure minime di sicurezza, come indicato nella lettera di designazione ad incaricato del trattamento dei dati

13.2 Gli strumenti tecnologici considerati nel presente Regolamento 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 e successive modifiche ed integrazioni; conseguentemente, le informazioni raccolte sulla base di quanto indicato nel Regolamento, anche conformemente al successivo punto 13, possono essere utilizzate a tutti i fini connessi al rapporto di lavoro, essendone stata data informazione ai lavoratori sulle modalità di uso degli strumenti stessi, sugli interventi che potranno venir compiuti nel sistema informatico ovvero nel singolo strumento e sui conseguenti sistemi di controllo che potessero venir eventualmente compiuti (conformemente al successivo punto 14), fermo restando il rispetto della normativa in materia di protezione dei dati personali (Reg. UE 679/2016).

13.3 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 loro utilizzo come strumenti per il controllo a distanza dell'attività dei lavoratori; peraltro, lì dove l'adozione di tali apparati risultasse necessaria per finalità altre, es. esigenze organizzative e produttive, di sicurezza del lavoro e/o di tutela del patrimonio provvederà conformemente a quanto disposto dall'art.4, comma primo, della Legge n.300/1970 e successive modifiche ed integrazioni, dandone anche opportuna informazione agli utenti stessi.

14 ACCESSO AI DATI TRATTATI DALL'UTENTE

14.1 Oltre che per motivi di sicurezza del sistema informatico, compresi i motivi tecnici e/o manutentivi (ad esempio, aggiornamento/sostituzione/implementazione di programmi, manutenzione hardware, etc.), per finalità di controllo e programmazione dei costi (ad esempio, verifica costi di connessione ad internet, traffico telefonico, etc.), comunque estranei a qualsiasi finalità di controllo dell'attività lavorativa, è facoltà del Responsabile Trattamento Dati, tramite il personale incaricato, accedere direttamente, nel rispetto della normativa sulla privacy e delle procedure di cui ai precedenti 4.3. e 4.4, a tutti gli strumenti informatici e ai documenti ivi contenuti, nonché ai tabulati del traffico telefonico.

15 SISTEMI DI CONTROLLI GRADUALI

15.1 In caso di anomalie, il personale incaricato effettuerà controlli anonimi che si concluderanno con avvisi generalizzati diretti ai dipendenti dell'area o del settore in cui è stata rilevata l'anomalia, nei quali si evidenzierà l'utilizzo irregolare degli strumenti e si inviteranno gli interessati ad attenersi scrupolosamente ai compiti assegnati e alle istruzioni impartite. Controlli su base più ristretta o anche individuale potranno essere compiuti solo in caso di successive ulteriori anomalie.

15.2 In nessun caso verranno compiuti controlli prolungati, costanti o indiscriminati.

16 SANZIONI

16.1 È fatto obbligo a tutti gli utenti di osservare le disposizioni portate a conoscenza con il presente Regolamento. Il mancato rispetto o la violazione delle regole sopra ricordate è perseguibile nei confronti del personale dipendente con provvedimenti disciplinari e risarcitori previsti dal vigente CCNL, e nei confronti dei collaboratori, consulenti ed incaricati esterni di cui all'1.2, verificata la gravità della violazione contestata, con la risoluzione od il recesso dal contratto ad essi relativo nonché con tutte le azioni civili e penali consentite.

17 AGGIORNAMENTO E REVISIONI

17.1 Tutti gli utenti possono proporre, quando ritenuto necessario, integrazioni motivate al presente Regolamento. Le proposte verranno esaminate dal Responsabile Trattamento Dati.

17.2 Il presente Regolamento è soggetto periodicamente a revisione.