CONSERVATORIO STATALE DI MUSICA
JACOPO TOMADINI UDINE

AMMINISTRAZIONE

REGOLAMENTO
PER L'UTILIZZO DEI
SISTEMI INFORMATICI
DA PARTE DI DIPENDENTI E COLLABORATORI

Approvato dal Consiglio di Amministrazione del 10/07/2019

Membro dell'Associazione
Europea dei Conservatori
e delle Accademie Musicali

P.zza 1° Maggio, 29
33100 Udine (Italia)
Codice fiscale 94005860302

t +39 0432 502755
f +39 0432 510740
www.conservatorio.udine.it

Indice

Aggiornamenti

Versione	Data	Cambiamenti effettuati dall'ultima versione
1.0	10/07/2019	Prima versione

Premessa

Questo documento è predisposto secondo uno schema condiviso tra il Conservatorio di Udine e di Trieste nell'ambito della consolidata collaborazione tra le due istituzioni, secondo la convenzione amministrativa rinnovata per il triennio 2019-2021 e sottoscritta dai presidenti delle due Istituzioni.

Il presente Regolamento intende fornire ai dipendenti e collaboratori, denominati anche incaricati o utenti, del Conservatorio di Udine (di seguito denominato *CONSUD*) le indicazioni per una corretta e adeguata gestione delle informazioni attraverso l'uso di sistemi, applicazioni e strumenti informatici di CONSUD.

Si specifica che tutti gli strumenti utilizzati dal lavoratore (es. PC, notebook, risorse, e-mail ed altri strumenti con relativi software e applicativi, di seguito più semplicemente "*Strumenti*") sono messi a disposizione da CONSUD nell'ambito del rapporto lavorativo.

Per "rete locale" si intende la rete locale a cui sono collegati i PC amministrativi.

Gli Strumenti, nonché le relative reti di CONSUD a cui è possibile accedere tramite gli stessi, sono domicilio informatico di CONSUD.

Nell'ambito del rapporto lavorativo i dati personali e le altre informazioni dell'Utente che sono registrati negli Strumenti o che si possono eventualmente raccogliere tramite il loro uso, sono utilizzati per finalità istituzionali, per esigenze organizzative e produttive, per la sicurezza del lavoro e del patrimonio di CONSUD, per la sicurezza informatica e la tutela del sistema informatico dello stesso.

Tali informazioni sono utilizzabili a tutti i fini connessi al rapporto di lavoro; il presente Regolamento costituisce adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli, nel rispetto di quanto disposto dal Regolamento Europeo 679/16 sulla protezione dei dati personali.

Si precisa che non sono installati o configurati sui sistemi informatici in uso agli utenti elementi aventi come scopo il controllo a distanza dell'attività dei lavoratori.

1 Campo di applicazione

1.1. Il presente regolamento si applica a tutti i dipendenti, senza distinzione di ruolo e/o di livello, nonché a tutti i collaboratori di CONSUD a prescindere dal rapporto contrattuale con lo stesso intrattenuto.

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

1.3. Il presente regolamento entra a far parte, per quanto di pertinenza, del Codice di comportamento del Conservatorio.

2. Oggetto e finalità

2.1. Il presente Regolamento è redatto:

- alla luce della Legge 20.5.1970, n. 300, recante "Norme sulla tutela della libertà e dignità dei lavoratori, della libertà sindacale e dell'attività sindacale nei luoghi di lavoro e norme sul collocamento";
- in attuazione del Regolamento Europeo 679/16 sulla protezione dei dati personali (d'ora in avanti Reg. 679/16 o GDPR);
- ai sensi delle "Linee guida del Garante per posta elettronica e internet" in Gazzetta Ufficiale n. 58 del 10 marzo 2007;
- alla luce dell'articolo 23 del D.Lgs. n. 151/2015 (c.d. Jobs Act) che modifica e rimodula la fattispecie integrante il divieto dei controlli a distanza, nella consapevolezza di dover tener conto, nell'attuale contesto produttivo, oltre agli impianti audiovisivi, anche degli altri strumenti *«dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori»* e di quelli *«utilizzati dal lavoratore per rendere la prestazione lavorativa».*

2.2. La finalità è quella di promuovere in tutto il personale dell'Ente una corretta "cultura informatica" nell'utilizzo degli Strumenti informatici e telematici forniti dall'Ente, quali la posta elettronica, internet e i personal computer con i relativi software, nell'ambito del rapporto lavorativo.

3. Principi generali e di riservatezza nelle comunicazioni

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

3.1.1. il principio di **necessità**, secondo cui i sistemi informativi e i programmi informatici devono essere impiegati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi in relazione alle finalità perseguite (art. 5 e 6 del Reg. 679/16);

3.1.2. il principio di **correttezza**, secondo cui le caratteristiche essenziali dei trattamenti devono essere rese note ai lavoratori. Le tecnologie dell'informazione (in modo più marcato rispetto ad apparecchiature tradizionali) permettono di svolgere trattamenti ulteriori rispetto a quelli connessi ordinariamente all'attività lavorativa. Ciò, all'insaputa o senza la piena consapevolezza dei lavoratori, considerate anche le potenziali applicazioni di regola non adeguatamente conosciute dagli interessati;

3.1.3. i trattamenti devono essere effettuati per **finalità determinate**, esplicite e legittime (art.5 commi 1 e 2), osservando il principio di pertinenza e non eccedenza. Il datore di lavoro deve trattare i dati "nella misura meno invasiva possibile"; le attività di monitoraggio devono essere svolte solo da soggetti preposti ed essere "mirate sull'area di rischio, tenendo conto della normativa sulla protezione dei dati e del principio di segretezza della corrispondenza".

3.2. Il dipendente si attiene alle seguenti regole di trattamento:

3.2.1. È vietato comunicare a soggetti non specificatamente autorizzati i dati personali comuni, sensibili, giudiziari, sanitari o altri dati, elementi e informazioni trattate da CONSUD 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.

3.2.2. 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.

3.2.3. È vietato lasciare incustoditi documenti, lettere, fascicoli, appunti e quant'altro possa contenere dati personali e/o informazioni di CONSUD quando il dipendente/collaboratore si allontana dalla postazione di lavoro. È vietato lasciare sulla postazione di lavoro (scrivania, bancone ecc.) materiali che non siano inerenti la pratica che si sta trattando in quel momento. Ciò vale soprattutto nel caso di lavoratori con mansioni di front office.

4. Tutela del lavoratore

4.1. Alla luce dell'art. 4, comma 1, L.n. 300/1970, la regolamentazione della materia indicata nel presente Regolamento, non è finalizzata all'esercizio di un controllo a distanza dei lavoratori da parte del datore di lavoro ma solo a permettere a quest'ultimo di utilizzare sistemi informativi per fare fronte ad esigenze produttive od organizzative e di sicurezza nel trattamento dei dati personali.

4.2. È garantito al singolo lavoratore il controllo sui propri dati personali secondo quanto previsto dagli articoli 15-16-17-18-20-21-78 del Reg. 679/16.

5. Gestione, assegnazione e revoca delle credenziali di accesso

5.1. Le credenziali di autenticazione per l'accesso alle risorse informatiche vengono assegnate al momento dell'assunzione o dell'affidamento dell'incarico.

5.2. Le credenziali di autenticazioni consistono in un codice per l'identificazione dell'utente (altresì nominati username, nome utente o user id) ed una relativa password. La password è personale e riservata e dovrà essere conservata e custodita dall'incaricato con la massima diligenza e non divulgata.

5.3. La password deve essere di adeguata robustezza: deve essere composta seguendo le regole definite dall'Amministratore del sistema.

5.4. È necessario procedere alla modifica della password a cura dell'utente al primo accesso e, successivamente, ad ogni scadenza proposta dal sistema.

5.5. Nel caso di cessazione del rapporto di lavoro con il dipendente/collaboratore, la procedura di chiusura rapporto prevede il blocco degli account di accesso alla rete interna di CONSUD, dell'account di posta elettronica, mantenendo la possibilità di accesso in sola lettura alle informazioni personali disponibili via Web dall'area riservata del sito.

6. Utilizzo della rete di CONSUD

6.1 Utilizzo della rete locale

6.1.1. Per l'accesso alle risorse informatiche di CONSUD attraverso la rete locale, ciascun utente deve essere in possesso di credenziali di autenticazione secondo l'art. 5.

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

6.1.3. L'accesso alla rete garantisce all'utente la disponibilità di condivisioni di rete (cartelle su server) nelle quali vanno inseriti e salvati i files di lavoro, organizzati per area/ufficio o per diversi criteri o per obiettivi specifici di lavoro, ed eventualmente di aree riservate allo specifico utente, sempre su server di rete.

6.1.4. Tutte le cartelle di rete, siano esse condivise o personali, possono ospitare esclusivamente contenuti professionali.

Tutte le risorse di memorizzazione diverse da quelle citate al punto precedente non sono sottoposte al controllo regolare degli Amministratori di Sistema e non sono oggetto di backup periodici. A titolo di esempio si citano: il disco C o altri dischi locali dei singoli PC, la cartella "Documenti" o "Desktop" dell'utente, gli eventuali dispositivi di memorizzazione locali o di disponibilità personale come Hard disk portatili o NAS ad uso esclusivo. Tutte queste aree di memorizzazione non devono ospitare dati di interesse di CONSUD, poiché non sono garantite la sicurezza e la protezione contro la eventuale perdita di dati. Pertanto, la responsabilità della disponibilità dei dati ivi contenuti è a carico del singolo utente.

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

6.1.6. Senza il consenso del Titolare è vietato salvare documenti elettronici di CONSUD su repository esterni (quali ad esempio Dropbox, GoogleDrive, OneDrive, ecc.) o inviarli a estranei non coinvolti nei processi di CONSUD via posta elettronica o con altri sistemi.

6.1.7. All'interno della sede di CONSUD è resa disponibile anche una rete senza fili "Wi-Fi". Tale rete consente l'accesso ad internet per i dispositivi non connessi alla rete LAN mediante cavo. L'accesso alla rete WiFi è concesso a utenti con credenziali riconosciute.

6.2 Accesso a Internet via WiFi

6.2.1 All'interno della sede di CONSUD è resa disponibile anche una rete senza fili "Wi-Fi". Tale rete consente l'accesso ad internet per i dispositivi non connessi alla rete LAN mediante cavo. L'accesso alla rete WiFi è concesso in base ad una preventiva autorizzazione dell'Amministratore di sistema, quindi a utenti con credenziali riconosciute sul circuito.

I log relativi all'uso della rete sono registrati e possono essere oggetto di controllo da parte del Titolare del trattamento per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio dell'Ente, secondo le modalità descritte al capitolo "Controlli sugli Strumenti". Questa nota costituisce adeguata informazione delle modalità di effettuazione dei controlli ai sensi del GDPR. Rivolgersi all'Amministratore di sistema per informazioni di dettaglio sulla registrazione dei log.

7 Utilizzo degli Strumenti elettronici

Con strumenti elettronici si intendono PC, notebook e altri strumenti con relativi software e applicativi messi a disposizione del lavoratore da parte di CONSUD.

7.1 Il dipendente/collaboratore è consapevole che gli Strumenti forniti sono di proprietà di CONSUD e devono essere utilizzati nell'ambito del rapporto lavorativo. Ognuno è responsabile dell'utilizzo delle dotazioni informatiche ricevute in assegnazione. Ciascun dipendente /collaboratore si deve quindi attenere alle seguenti regole di utilizzo degli Strumenti.

7.2 L'accesso agli Strumenti dei CONSUD è protetto da password; per l'accesso devono essere utilizzati Username e password assegnate dall'Amministratore di sistema. Si rammenta che essi sono strettamente personali e l'utente è tenuto a conservarli nella massima segretezza.

7.3 Il Personal Computer, notebook, tablet ed ogni altro hardware deve essere custodito con cura da parte degli assegnatari segnalando tempestivamente all'Amministratore di sistema ogni malfunzionamento e/o danneggiamento. Non è consentita l'attivazione della password d'accensione (BIOS).

7.4 Non è consentito all'utente modificare le caratteristiche hardware e software impostate sugli Strumenti assegnati.

7.5 L'utente è tenuto a scollegarsi dal sistema, o bloccare l'accesso, ogni qualvolta si assenti dal locale nel quale è ubicata la stazione di lavoro (PC): lasciare un PC incustodito connesso alla rete può essere causa di utilizzo da parte di terzi senza che vi sia la possibilità di provarne in seguito l'indebito uso. Sarà comunque installato uno screen saver a cura dell'Amministratore del Sistema: questo si attiva dopo alcuni minuti di non utilizzo e può essere disattivato solo su inserimento della password dell'utente.

7.6 Le informazioni archiviate sul PC locale necessarie all'attività lavorativa assegnata devono essere riportate sulle aree di rete sottoposte a backup al completamento del lavoro.

7.7 Non è consentita l'installazione di programmi diversi da quelli installati dall'amministratore di sistema.

7.8 L'Amministratore di sistema potrà in qualunque momento procedere alla rimozione di ogni file o applicazione che riterrà essere pericolosi per la sicurezza dei PC, della rete locale e dei server di CONSUD, nonché tutte le impostazioni eventualmente configurate che possano interferire con il corretto funzionamento dei servizi informatici di CONSUD.

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

7.10 È vietato utilizzare il PC per l'acquisizione, la duplicazione e/o la trasmissione illegale di opere protette da copyright.

7.11 L'utilizzo di supporti di memoria (chiavi USB, CD, DVD o altri supporti) per il salvataggio di dati trattati tramite gli Strumenti di CONSUD deve essere funzionale all'attività lavorativa e sottoposta alle cautele dovute, in base al presente regolamento.

7.12 La connessione al PC di qualsiasi periferica deve essere funzionale all'attività lavorativa e sottoposta alle cautele dovute, in base al presente regolamento.

7.13 È assolutamente vietato connettere alla rete locale qualsiasi dispositivo (PC esterni, router, switch, modem, etc.) non autorizzato preventivamente dall'Amministratore di Sistema.

7.14 Nel caso in cui l'utente dovesse notare comportamenti anomali del PC, l'utente stesso è tenuto a comunicarlo tempestivamente all'Amministratore di Sistema.

I log relativi all'uso degli Strumenti, dei Server, dei file in essi trattati, sono registrati e possono essere oggetto di controllo da parte del Titolare del trattamento per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio dell'Ente, , secondo le modalità descritte al capitolo "Controlli sugli Strumenti". Questa nota costituisce adeguata informazione delle modalità di effettuazione dei controlli ai sensi del GDPR. Rivolgersi all'Amministratore di sistema per informazioni di dettaglio sulla registrazione dei log.

8 Utilizzo di internet

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 della rete Internet e dei relativi servizi.

8.1 La navigazione in internet deve essere funzionale all'attività lavorativa.

8.2 È vietato a chiunque il download di qualunque tipo di software gratuito (freeware) o shareware prelevato da siti Internet, se non espressamente autorizzato dagli Amministratori di Sistema.

8.3 CONSUD si riserva di bloccare l'accesso a siti "a rischio" attraverso l'utilizzo di blacklist pubbliche in continuo aggiornamento e di predisporre filtri, basati su sistemi euristici di valutazione del livello di sicurezza dei siti web remoti, tali da prevenire operazioni potenzialmente pericolose o comportamenti impropri. In caso di blocco accidentale di siti di interesse di CONSUD, contattare l'Amministratore di Sistema per uno sblocco selettivo.

8.4 È assolutamente vietato l'utilizzo di abbonamenti privati (ad esempio, chiavette internet installate sui PC del conservatorio) per effettuare la connessione a Internet bypassando i criteri di sicurezza impostati sulla rete istituzionale, tranne in casi del tutto eccezionali e previa autorizzazione degli Amministratori di Sistema.

8.5 È assolutamente vietata la partecipazione a Forum non professionali, ai Social Network, l'utilizzo di chat line, di bacheche elettroniche e le registrazioni in guest books anche utilizzando pseudonimi (o nicknames) per finalità non correlate alle attività lavorative.

8.6 È consentito l'uso di strumenti di messaggistica istantanea, per permettere una efficace e comoda comunicazione tra i colleghi, mediante i soli strumenti autorizzati dall'Amministratore di Sistema. Tali strumenti hanno lo scopo di migliorare la collaborazione tra utenti aggiungendo un ulteriore canale comunicativo rispetto agli spostamenti fisici, alle chiamate telefoniche ed e-mail.

Si informa che al fine di garantire il Servizio Internet e la sicurezza dei sistemi informativi, per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio, CONSUD mantiene i dati di navigazione registrati (file di log riferiti al traffico web). Tali dati potranno essere usati in forma aggregata per monitoraggio sull'utilizzo della rete. 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. secondo le modalità descritte al capitolo "Controlli sugli Strumenti". Questa nota costituisce adeguata informazione delle modalità di effettuazione dei controlli ai sensi del GDPR. Rivolgersi all'Amministratore di sistema per informazioni di dettaglio sulla registrazione dei dati di navigazione.

9 Utilizzo della posta elettronica

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

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

9.1 Ad ogni utente viene fornito un account e-mail di CONSUD. L'utente a cui è assegnata una casella di posta elettronica è responsabile del corretto utilizzo della stessa.

9.2 CONSUD fornisce, altresì, delle caselle di posta elettronica associate a ciascuna unità organizzativa, ufficio o gruppo di lavoro il cui utilizzo è da preferire rispetto alle e-mail nominative qualora le comunicazioni siano di interesse collettivo: questo per evitare che degli utenti singoli mantengano l'esclusività su dati di CONSUD.

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

9.4 Allo scopo di garantire sicurezza alla rete di CONSUD, evitare di aprire messaggi di posta in arrivo con contenuto sospetto o insolito, oppure che contengano allegati di tipo *.exe, *.com, *.vbs, *.htm, *.scr, *.bat, *.js e *.pif e ogni altra estensione non riconosciuta. È necessario porre molta attenzione, inoltre, ai link contenuti nel messaggio e alla credibilità del messaggio e del mittente, anche se conosciuto, per evitare casi di phishing o frodi informatiche. In qualunque situazione di incertezza contattare gli Amministratori di Sistema per una valutazione dei singoli casi.

9.5 Non é consentito diffondere messaggi del tipo "catena di S. Antonio" o di tipologia simile anche se il contenuto sembra meritevole di attenzione; in particolare gli appelli di solidarietà e i messaggi che informano dell'esistenza di nuovi virus. In generale è vietato l'invio di messaggi pubblicitari di prodotti di qualsiasi tipo.

9.6 Nel caso fosse necessario inviare allegati "pesanti" (fino al 10 MB) è opportuno ricorrere prima alla compressione dei file originali in un archivio di formato .zip o equivalenti. Nel caso di allegati ancora più voluminosi è necessario rivolgersi all'Amministratore di Sistema.

9.7 Nel caso in cui fosse necessario inviare a destinatari esterni messaggi contenenti allegati con dati personali sensibili, è obbligatorio che questi allegati vengano preventivamente resi inintelligibili attraverso crittazione con apposito software (archiviazione e compressione con password). La password di crittazione deve essere comunicata al destinatario attraverso un canale diverso dalla mail (ad esempio per telefono) e mai assieme ai dati criptati.

9.8 Non è consentito l'invio automatico di e-mail all'indirizzo e-mail privato (attivando per esempio un "inoltro" automatico delle e-mail entranti), anche durante i periodi di assenza (es. ferie, malattia, infortunio ecc.). In questa ultima ipotesi, è raccomandabile utilizzare un messaggio "Out of Office" facendo menzione di chi, all'interno di CONSUD, assumerà le mansioni durante l'assenza, oppure indicando un indirizzo di mail alternativo preferibilmente di tipo collettivo, tipo ufficio….@conservatorio.udine.it. Rivolgersi all'Amministratore di Sistema per tale eventualità.

9.9 In caso di assenza improvvisa o prolungata e per improrogabili necessità legate all'attività lavorativa per l'utilizzo delle caselle d'ufficio, è prevista la sostituzione da parte del personale in servizio.

9.10 La diffusione massiva di messaggi di posta elettronica deve essere effettuata esclusivamente per motivi inerenti il servizio. I destinatari dovranno essere messi in copia nascosta (Bcc o Ccn) se la tipologia del messaggio lo consente.

9.11 È vietato inviare posta elettronica in nome e per conto di un altro utente, salvo sua espressa autorizzazione.

9.12 Il contenuto delle caselle di posta elettronica tipo ufficio….@conservatorio.udine.it è periodicamente salvato in locale.

9.13 Sono fornite, altresì, utenze personali nome.cognome@conservatorio.udine.it, assegnate per esclusiva corrispondenza istituzionale che al termine del rapporto di lavoro vengono cancellate.

9.14 I messaggi in entrata vengono sistematicamente analizzati alla ricerca di virus e malware e per l'eliminazione dello spam. I messaggi che dovessero contenere virus vengono eliminati dal sistema e il mittente/destinatario viene avvisato mediante messaggio specifico.

10 Utilizzo dei telefoni, fax, fotocopiatrici, scanner e stampanti dell'Ente

Il dipendente è consapevole che gli Strumenti di stampa, così come anche il telefono di CONSUD, sono di proprietà dello stesso e sono resi disponibili all'utente per rendere la prestazione lavorativa. Pertanto, ne viene concesso l'uso esclusivamente per tale fine.

10.1 Il telefono di CONSUD affidato all'utente è uno strumento di lavoro. Ne viene concesso l'uso esclusivamente per lo svolgimento dell'attività lavorativa e non sono quindi consentite comunicazioni a carattere personale e/o non strettamente inerenti l'attività lavorativa stessa. La ricezione o l'effettuazione di comunicazioni a carattere personale è consentito solo nel caso di comprovata necessità ed urgenza.

10.2 Qualora venisse assegnato un cellulare di CONSUD all'utente, quest'ultimo sarà responsabile del suo utilizzo e della sua custodia. Ai cellulari e smartphone di CONSUD si applicano le medesime regole sopra previste per gli altri dispositivi informatici (cfr. 7 "Utilizzo di personal computer"), per quanto riguarda il mantenimento di un adeguato livello di sicurezza informatica. In particolare, si raccomanda il rispetto delle regole per una corretta navigazione in Internet (cfr. 8), se consentita.

10.3 Per gli smartphone di CONSUD è vietata l'installazione e l'utilizzo di applicazioni (o altresì denominate "app" nel contesto degli smartphone) diverse da quelle autorizzate Amministratore di Sistema.

10.4 È vietato l'utilizzo delle fotocopiatrici di CONSUD per fini personali.

10.5 Per quanto concerne l'uso delle stampanti gli utenti sono tenuti a:

10.5.1 Stampare documenti solo se strettamente necessari per lo svolgimento delle proprie funzioni operative

10.5.2 Prediligere le stampanti di rete condivise, rispetto a quelle locali/personali, per ridurre l'utilizzo di materiali di consumo (toner ed altri consumabili)

10.5.3 Prediligere la stampa in bianco/nero e fronte/retro al fine di ridurre i costi, se possibile.

10.6 Le stampanti e le fotocopiatrici di CONSUD devono essere spente ogni sera prima di lasciare gli uffici o in caso di inutilizzo prolungato.

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

11 Utilizzo di dispositivi propri in modalità BYOD

Qualora un incaricato/autorizzato sia stato espressamente autorizzato dal Conservatorio all'utilizzo di dispositivi elettronici personali durante le attività lavorative, premesso che il Conservatorio è "Titolare del trattamento" relativamente ai dati che sono trattati per suo conto da parte dell'incaricato/autorizzato al trattamento, occorre che si uniformi alle sottostanti prescrizioni, pena l'applicazione di sanzioni.

11.1 i dati personali degli interessati non devono essere trattati per scopi differenti da quelli per cui sono stati originariamente raccolti e devono essere utilizzati solo per il tempo necessario

11.2 deve essere assolutamente evitata la disseminazione indistinta (ad esempio su più dispositivi) dei dati personali oggetto di trattamento tramite BYOD

11.3 l'accesso ai dispositivi deve essere regolamentato da apposite credenziali (es: password o PIN). Il dispositivo deve essere adeguatamente protetto da antivirus/firewall locali costantemente aggiornati.

11.4 qualora il dispositivo personale che contiene dati del Titolare del trattamento, fosse perso, smarrito, rubato, fosse oggetto di un accesso improprio o comunque ci sono elementi per immaginare/sospettare che i dati contenuti possano essere, sia pure temporaneamente, resi accessibili a terze parti, l'incaricato/autorizzato deve informare immediatamente il Titolare del trattamento affinché possa essere valutata la problematica e prese, se del caso le opportune misure. La comunicazione deve essere immediata e non possono esser accettati ritardi

11.5 nel caso in cui il dispositivo mobile del lavoratore sia venduto, ceduto, trasferito, il contenuto deve essere cancellato/anonimizzato in modo irreversibile

Per ogni azione di cui ai punti 11.4), 11.5), il Referente interno del Sistema Informativo è disponibile a riguardo.

12 Assistenza agli utenti e manutenzioni

12.1 Gli Amministratori di Sistema e i Responsabili Esterni Autorizzati possono accedere ai dispositivi informatici di CONSUD sia direttamente, sia mediante software di accesso remoto, per i seguenti scopi:

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

aggiornamento software e manutenzione preventiva hardware e software.

Gli interventi tecnici posso avvenire previo consenso dell'utente, quando l'intervento stesso richiede l'accesso ad aree personali dell'utente stesso. Qualora l'intervento tecnico in loco o in remoto non necessiti di accedere mediante credenziali utente, gli Amministratori di sistema sono autorizzati ad effettuare gli interventi senza il consenso dell'utente cui la risorsa è assegnata.

12.2 L'accesso in teleassistenza sui PC della rete di CONSUD richiesto da terzi (fornitori e/o altri) deve essere autorizzato dall'Amministratore di Sistema, per le verifiche delle modalità di intervento per il primo accesso. Le richieste successive, se effettuate con la medesima modalità, possono essere gestite autonomamente dall'utente finale.

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

13 Controlli sugli Strumenti

In caso di anomalie l'amministratore di sistema, le segnalerà al Referente interno del sistema informativo, cui compete l'eventuale attivazione di controlli anonimi che si concluderanno con avvisi generalizzati diretti ai dipendenti nei quali si evidenzierà l'utilizzo irregolare degli strumenti e si inviterà il personale ad attenersi scrupolosamente ai compiti assegnati ed alle istruzioni impartite. Controlli su base più ristretta od individuale potranno essere compiuti, secondo la medesima procedura, solo in caso di successive ulteriori anomalie.
In nessun caso verranno compiuti controlli prolungati, costanti o indiscriminati.
Il controllo sugli strumenti è previsto dall'art. 6.1 Provv. Garante, ad integrazione dell'Informativa ex art. 13 Reg. 679/16.

14 Partecipazioni a Social Media

14.1 L'utilizzo a fini promozionali di Facebook, Twitter, Linkedin, dei blog e dei forum, anche professionali (ed altri siti o social media) è gestito ed organizzato esclusivamente da CONSUD. Rimanendo escluse iniziative individuali da parte dei singoli utenti non autorizzati. È vietata la partecipazione a titolo privato agli stessi social media durante l'orario di lavoro.

14.2 Fermo restando il diritto della persona alla libertà di espressione, CONSUD ritiene comunque opportuno indicare agli utenti alcune regole comportamentali, al fine di tutelare tanto la propria immagine ed il patrimonio di CONSUD, anche immateriale, quanto i propri collaboratori, i propri clienti e fornitori, gli altri partners, oltre che gli stessi utenti utilizzatori dei social media.

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

14.4 La condivisione dei contenuti nei social media deve sempre rispettare e garantire la segretezza sulle informazioni di CONSUD, nel rispetto del segreto d'ufficio, segreto professionale e privacy.

15 Disposizioni finali

15.1 Sanzioni

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 in esso riportate è perseguibile nei confronti del personale dipendente con provvedimenti disciplinari previsti dal vigente CCNL, e nei confronti dei collaboratori, verificata la gravità della violazione contestata, con la risoluzione del contratto ad essi relativo, nonché con tutte le azioni civili e penali consentite.

15.2 Aggiornamenti

Il Presente Regolamento sarà soggetto a revisioni periodiche ogniqualvolta questo sia necessario a seguito di modifiche tecniche, organizzative e/o normative che ne richiedano l'aggiornamento.

15.3 Pubblicazione

Il presente regolamento è pubblicato sul sito istituzionale www.conservatorio.udine.it nella sezione Il Conservatorio/Organizzazione/Statuto e Regolamenti.

Data 10/07/2019

Firma del titolare o responsabile del trattamento

Il Direttore
M.o Virginio Pio Zoccattelli
Firma autografa sostituita a mezzo stampa
ai sensi dell'art. 3, comma 2 del d.lgs. n. 39 del 1993