Conservatorio
Arrigo Boito di Parma

IL PRESIDENTE

VISTA la Legge n. 508 del 21/12/1999 di riforma delle Accademie di belle Arti, dell'Accademia Nazionale di Danza, dell'Accademia nazionale di Arte Drammatica, degli Istituti Superiori per le Industrie Artistiche, dei Conservatori di Musica e degli Istituti Musicali Pareggiati;

VISTO il D.P.R. n. 132 del 28/02/2003 riguardante il regolamento recante criteri per l'autonomia statutaria, regolamentare ed organizzativa delle Istituzioni Artistiche e Musicali, ai sensi della Legge. n. 508/1999;

VISTO lo Statuto del Conservatorio Arrigo Boito di Parma;

VISTA la delibera del 15 settembre 2025con la quale il Consiglio Accademico ha dato parere positivo all'adozione del " Regolamento per l'utilizzo dei sistemi informatici";

VISTA la delibera del 18 settembre con la quale il Consiglio di Amministrazione ha approvato il "Regolamento per l'utilizzo dei sistemi informatici";

Ritenuto necessario procedere all'emanazione del suddetto regolamento;

ADOTTA

Il Regolamento per l'utilizzo dei sistemi informatici - approvato a seguito di delibera del 18 settembre 2025 del Consiglio di Amministrazione del Conservatorio Arrigo Boito, allegato al presente atto.

Il Regolamento sarà pubblicato presso la sezione Amministrazione Trasparente del sito internet ufficiale del Conservatorio di Parma (www.conservatorio.pr.it).

Il Presidente
Prof. Marco Ferretti

Marco
Ferretti
06.10.2025
10:21:16
GMT+02:00

REGOLAMENTO PER L'UTILIZZO DEI SISTEMI INFORMATICI DEL CONSERVATORIO "A. BOITO" DI PARMA

Art. 1 - Premessa

Di fronte all'innegabile difficoltà che hanno i Conservatori di controllare il corretto uso da parte dei propri dipendenti del personal computer e dei relativi programmi, nonché il rispetto della riservatezza alla quale tutti i soggetti sono tenuti, vi è il rischio che tali controlli possano essere insufficienti, o perfino considerati illegittimi ai sensi dello statuto dei lavoratori.

La progressiva diffusione delle tecnologie informatiche, ed in particolare l'accesso alla rete Internet dai PC istituzionali, espone il ***CONSERVATORIO DI MUSICA "ARRIGO BOITO"*** di seguito definita come "Istituzione", a rischi di un coinvolgimento sia patrimoniale che penale, creando problemi alla sicurezza e all'immagine stessa del *Conservatorio di Musica "Arrigo Boito".*

In particolare, accessi abusivi alla rete informatica del *Conservatorio di Musica "Arrigo Boito"* possono comportare danni, anche irreparabili, al funzionamento del sistema informatico e dei software e pregiudicare la sicurezza dei dati conservati, oltre a comportare un pericolo per la loro integrità e segretezza, con conseguente lesione dei diritti patrimoniali e di proprietà, anche intellettuale, del *Conservatorio di Musica "Arrigo Boito"* e di terzi in qualsiasi modo ad essa collegati

Premesso quindi che l'utilizzo delle risorse informatiche e telematiche deve sempre ispirarsi al principio della diligenza e correttezza, il *Conservatorio di Musica "Arrigo Boito"* adotta un Regolamento interno diretto ad evitare che comportamenti inconsapevoli possano innescare problemi o minacce alla sicurezza nel trattamento dei dati.

L'adozione di un regolamento Istituzionale ha lo scopo di limitare l'uso improprio di tali strumenti di lavoro e la conseguente responsabilità del *Conservatorio di Musica "Arrigo Boito"*, nonché di rispettare quanto previsto dalla normativa sulla Privacy.

Tutti i dipendenti ed i collaboratori, nonché coloro che anche saltuariamente o per periodi limitati, in forza di appositi contratti o convenzioni o per lavoro in regime di somministrazione, sono impiegati presso il *Conservatorio di Musica "Arrigo Boito"* (d'ora innanzi indicati anche semplicemente come "il lavoratore" o "il dipendente" o il "personale" o l'"utente"), sono tenuti al rispetto delle disposizioni impartite dalle seguenti Linee guida.

Art. 2 - Utilizzo del Personal Computer/Notebook

1. L'utente è l'unico responsabile di tutti gli strumenti e/o delle dotazioni ricevute in uso dal *Conservatorio di Musica "Arrigo Boito"*, siano essi PC fissi, PC portatili e relative borse/valige porta computer, accessori PC (tastiere, mouse, Hard disk esterni, chiavi USB, …), supporti magnetici ed ottici, Smartphone e Tablet in genere, Navigatori Satellitari, Macchine fotografiche, videocamere. Egli deve custodirli con estrema cura e diligenza sia durante il loro utilizzo che durante gli spostamenti.
2. Ogni utilizzo non inerente all'attività lavorativa può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza dei dati pertanto è vietato l'utilizzo privato del notebook.
3. Non è consentita l'attivazione della password d'accensione senza preventiva autorizzazione da parte del *Conservatorio di Musica "Arrigo Boito"*.
4. Sulla rete Istituzionale gli utenti sono configurati secondo il principio LPA (*Least Privileged Account*). Pertanto, sui PC Istituzionali gli utenti hanno i privilegi di accesso normalmente consentiti al gruppo *User*.
5. Non è consentito effettuare il download, copiare, installare autonomamente programmi provenienti dall'esterno salvo preventiva autorizzazione esplicita del *Conservatorio di Musica "Arrigo Boito"*. Ciò è indispensabile per evitare di alterare la stabilità delle applicazioni dell'elaboratore e soprattutto per la conseguente responsabilità civile e penale che verrebbe ad incombere sul *Conservatorio di Musica "Arrigo Boito"*.
6. Non è consentito l'utilizzo di software per il quale il *Conservatorio di Musica "Arrigo Boito"* non sia in possesso della regolare licenza d'uso.
7. La configurazione hardware e software dei PC del *Conservatorio di Musica "Arrigo Boito"*, così come le modalità di utilizzo degli stessi, viene determinata dal Servizio ICT sulla base delle indicazioni della Direzione e delle esigenze e necessità dei singoli servizi in relazione all'attività Istituzionale.
8. Per quanto indicato al precedente punto non è consentito l'uso di programmi diversi da quelli installati ufficialmente dal *Conservatorio di Musica "Arrigo Boito"*.
9. Non è consentito all'utente modificare le caratteristiche di configurazione impostate sul PC a lui assegnato salvo preventiva autorizzazione esplicita da parte del *Conservatorio di Musica "Arrigo Boito"*.
10. È espressamente vietato intervenire sui collegamenti, siano essi elettrici o di rete dati. Il Servizio ICT dovrà essere tempestivamente informato in caso si rendesse necessario un intervento di questo tipo.
11. Il PC ed il monitor devono essere spenti ogni sera prima di lasciare gli uffici.
12. In caso di assenze prolungate dalla Stazione di Lavoro, nell'ambito della giornata lavorativa, l'utente deve assicurarsi di aver chiuso tutte le applicazioni ed i file aperti; se la postazione di lavoro rimane temporaneamente incustodita, deve essere bloccato l'accesso all'elaboratore con cui si trattano i dati utilizzando la funzione *Blocca Computer* disponibile.
13. Non è consentita la connessione e l'installazione sul proprio PC di dispositivi di memorizzazione, di sistemi di comunicazione o di altro (masterizzatori, scanner, modem, lettori MP3, ecc.) se non con la preventiva autorizzazione da parte del *Conservatorio di Musica "Arrigo Boito"*.
14. Le informazioni archiviate informaticamente devono essere esclusivamente quelle necessarie all'attività lavorativa e compatibili con il Regolamento 2016/679 e il D. Lgs.101/2018 in materia di privacy.
15. Non è consentita la memorizzazione di documenti informatici di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica.
16. Costituisce buona regolala pulizia periodica (almeno ogni sei mesi) degli archivi, con cancellazione dei file obsoleti o inutili. Particolare attenzione deve essere prestata alla duplicazione dei dati per evitare un'archiviazione ridondante.
17. I PC portatili utilizzati all'esterno, in caso di allontanamento, devono essere custoditi in luogo protetto.

18. Le attività lavorative devono essere svolte tramite l'utilizzo esclusivo di device Istituzionali. È comunque vietato l'uso di supporti di archiviazione removibili per la memorizzazione dei dati particolari (Ex. Art. 9 Reg. UE 679/2016) se non protetti da password.

Art. 3 - Utilizzo della rete interna

1. Le unità di rete 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 periodi brevi, su queste unità.
2. È espressamente vietato condividere file o cartelle dal proprio PC.
3. Il Servizio ICT può in qualunque momento procedere alla rimozione di ogni file o applicazione che riterrà essere pericoloso per la sicurezza sia sui PC degli utenti sia sulle unità di rete.
4. È vietato definire cartelle in rete dotate di password, se non dietro esplicita e formale autorizzazione del responsabile di riferimento.

Art. 4 - Gestione delle password

1. Ad ogni utente abilitato all'utilizzo del Sistema Informatico Istituzionale vengono assegnate le Credenziali di Autenticazione composte da username e password.
2. Le Credenziali di Autenticazione (username e password) devono essere custodite dall'incaricato gelosamente e con la massima diligenza al fine di evitare il furto o lo smarrimento delle stesse. Le credenziali sono valide per l'accesso al Sistema Informatico Istituzionale.
3. L'utente è tenuto a conservare nella massima segretezza la parola di accesso alla rete ed ai sistemi e qualsiasi altra informazione legata al processo di autenticazione.
4. La password deve essere immediatamente sostituita, dandone comunicazione al proprio referente, nel caso si sospetti che abbia perso segretezza.
5. Le Credenziali di Accesso al Sistema Informatico Istituzionale sono strettamente personali, non è quindi consentito accedere al sistema informatico utilizzando credenziali di altri utenti.
6. La password di accesso alla rete deve essere modificata al primo accesso al sistema ed è stabilita direttamente dall'utente. Nella definizione della stessa occorre rispettare i seguenti requisiti di complessità:
    a. non può contenere più di due caratteri consecutivi del nome completo dell'utente o del nome dell'account utente;
    b. non deve contenere riferimenti riconducibili all'utente;
    c. deve includere almeno otto caratteri;
    d. deve contenere caratteri appartenenti ad almeno tre delle quattro categorie seguenti:
        i. caratteri maiuscoli dell'alfabeto inglese (A-Z)
        ii. caratteri minuscoli dell'alfabeto inglese (a-z)
        iii. numeri (0-9) iv. caratteri non alfabetici, ad esempio !, $, #, %
7. La durata massima della password è stabilita in 365 giorni di calendario.
8. Il numero di nuove password univoche che devono essere associate ad un account utente prima che sia possibile riutilizzare una vecchia password è 5 (cinque).
9. In prossimità della scadenza un messaggio automatico ricorderà all'utente la necessità di inserire una nuova password.
10. La durata minima della password è stabilita in 1 giorno di calendario
11. La password deve essere immediatamente sostituita nel caso si sospetti che la stessa abbia perso la segretezza.
12. Sui PC Istituzionali non è consentita l'attivazione della password di accensione (BIOS) senza preventiva autorizzazione da parte del Servizio ICT.

13. Qualora l'utente venisse a conoscenza delle password di altro utente, è tenuto a darne immediata notizia al Servizio ICT.
14. Il Profilo Utente verrà disattivato immediatamente in caso di cessazione del rapporto di lavoro. Successivamente alla cessazione del suddetto rapporto tutta la documentazione informatica, la corrispondenza elettronica ed i documenti allegati archiviati in rete e sui supporti fissi (hard disk/server) o mobili (storage, cd, etc.) si intenderanno relativi all'attività svolta dall'Utente tramite gli strumenti informatici e, pertanto, di esclusiva proprietà del *Conservatorio di Musica "Arrigo Boito"*, la quale potrà liberamente accedervi e/o utilizzarli nell'esercizio della propria attività. Resta inteso che, anche successivamente alla cessazione del rapporto lavorativo, l'utente può esercitare i diritti previsti dagli articoli da 15 a 22 del Regolamento (UE) 2016/679.

Art. 5 -Utilizzo dei supporti magnetici e personal cloud

1. Tutti i supporti magnetici ed ottici riutilizzabili contenenti dati sensibili devono essere trattati con particolare cautela onde evitare che il loro contenuto possa essere recuperato da personale non autorizzato.
2. Non è consentito scaricare files contenuti su supporti magnetici e/o ottici non aventi alcuna attinenza con la propria prestazione lavorativa.
3. I supporti rimovibili, hard disk esterni, supporti USB "chiavette", CD e DVD riscrivibili, memorie a stato solido, si contraddistinguono per un ingombro ed un peso contenuto; sono strumenti importanti, ormai divenuti di uso comune ed in grado di supportare (se correttamente utilizzati) l'efficacia dell'infrastruttura IT. L'utilizzo sistemi di personal storage o di supporti rimovibili deve essere espressamente autorizzato dalla Direzione e/o dall'Ufficio ICT.
4. Inoltre:

   a. ancorché autorizzati, agli utenti è consentito caricare sul o sui dispositivi rimovibili solamente i dati essenziali allo svolgimento del proprio lavoro;
   b. in caso di furto o smarrimento dispositivi rimovibili, gli utenti hanno l'obbligo di avvisare immediatamente il Servizio ICT;
   c. se un utente sospetta che sia stato effettuato un accesso non autorizzato ai dati, ha il dovere di riferirlo immediatamente;
   d. è preferibile dotare i dispositivi in parola di adeguate procedure di autenticazione (es: password) per l'accesso alle informazioni;
   e. è proibito scaricare sui dispositivi in parola copie pirata di software, o contenuti illegali. Tutti i dispositivi di archiviazione contenenti dati sensibili devono essere trattati con particolare cautela onde evitare che il loro contenuto possa essere recuperato o cadere in mano a terzi non autorizzati. La semplice cancellazione dei supporti non garantisce l'eliminazione dei dati in essi memorizzati; una persona esperta potrebbe infatti recuperare i dati memorizzati anche dopo la loro cancellazione. Supporti magnetici o tabulati, contenenti dati sensibili devono essere custoditi in archivi, cassetti chiusi a chiave.
   f. L'utilizzo di servizi di "personal cloud", diversi da quelli forniti dal *Conservatorio di Musica "Arrigo Boito"* (OFFICE 365 e GOOGLE WORKSPACE), che offrono un servizio di file hosting, sincronizzazione automatica di file e loro condivisione tramite web (es: Dropbox, iCloud, Sendspace, ecc.) è espressamente vietato dal *Conservatorio di Musica "Arrigo Boito"*.
   g. I servizi di cloud forniti dal *Conservatorio di Musica "Arrigo Boito"* devono essere utilizzati con l'autenticazione multifattore.

Art. 6 - Utilizzo di pc portatili

1. L'utente è responsabile del PC portatile ed eventuali accessori a lui assegnati in consegna e dotazione dal Servizio ICT; egli deve custodirlo con diligenza sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro.
2. Il PC portatile viene fornito per lo svolgimento dell'attività lavorativa e di conseguenza si applicano le regole di utilizzo previste per i PC connessi in rete (paragrafo UTILIZZO DEL PC ISTITUZIONALE).
3. Il PC portatile, solo per ragioni collegate allo svolgimento del proprio lavoro, può essere utilizzato all'esterno della sede Istituzionale; in tale caso si dovrà prestare adeguata cura ed attenzione per garantire la conservazione dello strumento verificandone la periodica disattivazione e la custodia in un luogo protetto. Ove possibil e salvo ragioni tecniche che ne impediscono l'attivazione, dovrà essere attivato il BITLOCKER, sistema di cifratura dei dati.
4. In caso di furto, smarrimento o danneggiamento in cui si rilevi incuria o negligenza dell'utente, potrà essere richiesto il risarcimento del danno causato al Conservatorio di Musica "Arrigo Boito".

Art. 7 - Utilizzo di mobile device

1. Qualora venisse assegnato un cellulare/smartphone Istituzionale all'utente, quest'ultimo sarà responsabile del suo utilizzo e della sua custodia. Anche ai mobili devices (smartphone/tablet) assegnati dal Conservatorio di Musica "Arrigo Boito" si applicano le prescrizioni del presente regolamento, con particolare cautela per le criticità insite negli strumenti in oggetto. In particolare, si richiede di: non modificare le impostazioni di sistema; segnalare immediatamente al Servizio ICT eventuali anomalie; prestare particolare attenzione alla custodia dello strumento e segnalare immediatamente lo smarrimento o il furto; prestare attenzione all'utilizzo in luoghi pubblici in cui potrebbero essere intercettate informazioni; evitare di collegare lo strumento a dispositivi non Istituzionali. Al fine di limitare i suddetti rischi, il Servizio ICT si riserva (comunicandolo agli utilizzatori) di utilizzare, anche attraverso strumenti di Mobile Device Management, apposite funzionalità tra cui:

a. attivazione PIN della SIM Card
b. attivazione di ulteriori procedure di autenticazione (ad applicazioni o supporti di memoria)
c. impostazione di prestabiliti tempi di session time-out
d. definizione di apposite politiche di back-up
e. attivazione delle funzionalità di aggiornamento automatico dei sistemi operativi e dei programmi anti-malware
f. attivazione delle procedure di remote-wiping da utilizzare in caso di smarrimento/furto del dispositivo
g. attivazione delle funzionalità di cifratura automatica dei dati
h. sistemi di controllo delle applicazioni installabili (c.d. white list)
i. sistemi di blocco navigazione e tracciatura attività
j. sistemi di geolocalizzazione dello strumento

2. Inoltre, è vietato l'utilizzo dello smartphone messo a disposizione per inviare o ricevere messaggistica elettronica (SMS, MMS, WhatsApp, ecc.) di natura personale o comunque non pertinenti rispetto allo svolgimento dell'attività lavorativa. L'eventuale uso promiscuo (per fini personali) di smartphone Istituzionale è possibile soltanto in caso di necessità comprovata e sempre in presenza di preventiva autorizzazione del responsabile di funzione e in conformità delle istruzioni al riguardo impartite tramite il presente o altri regolamenti Istituzionali. Eventuali regole specifiche per l'utilizzo dei mobile device potranno essere esplicitate nella modulistica di assegnazione degli strumenti agli utenti.

3. L'utilizzo della funzione di tethering (condivisione dell'accesso Internet) disponibile sui moderni mobile devices è espressamente vietato fatta eccezione per l'utilizzo tramite telefono Istituzionale in dotazione

Art. 8 - Utilizzo di mobile device personali

1. È fatto divieto l'utilizzo del device/smartphone personale durante le ore di lavoro, se non in casi di comprovata necessità e comunque non in maniera sistematica.
2. È vietato introdurre ed utilizzare in Istituzione, personal computer o altre apparecchiature elettroniche personali, se non preventivamente autorizzati dalla Direzione Istituzionale e/o dal Servizio ICT.
3. È consentito il collegamento esclusivamente alla rete wi-fi Guest.
4. È espressamente vietato il collegamento alla rete WIFI degli uffici
5. La configurazione dell'account di posta elettronica Istituzionale su device personali deve essere autorizzata dal responsabile di riferimento e comporta la necessità di utilizzo di sistemi di sicurezza all'accensione o di sblocco (PIN).

Art. 9 - Utilizzo di altri apparati Istituzionali e strumenti di connettività

1. Stampanti

Le stampe dimenticate possono spesso costituire involontaria fuga di notizie. Si raccomanda quindi la massima attenzione nell'utilizzo delle stampanti, con particolare riferimento alla corretta distruzione di documenti che non servono più. È cura dell'utente effettuare la stampa dei dati solo se strettamente necessaria e di ritirarla prontamente dai vassoi delle stampanti comuni. È necessario prestare la massima attenzione all'eventuale riutilizzo di stampe (carta da riciclo): tale pratica è di norma autorizzata solo quando i documenti contengano dati non personali pubblici.

2. Strumenti per disporre attività specifiche

Gli strumenti hardware necessari all'effettuazione di specifiche operazioni (dispositivi e card per la firma digitale, token per operazioni bancarie, ecc.) devono essere utilizzati esclusivamente dagli utenti espressamente identificati ed autorizzati. Tali utenti sono responsabili del corretto utilizzo di tali strumenti e devono preoccuparsi di:

- non consentirne l'accesso e l'utilizzo a soggetti non autorizzati;
- riporli alla fine dell'utilizzo (che deve essere il più possibile limitato nel tempo) nelle posizioni idonee;
- adottare tutti gli accorgimenti atti a prevenirne il furto o lo smarrimento.

Rientrano nelle medesime prescrizioni gli strumenti di registrazione degli accessi e delle presenze

3. Documenti cartacei

Tutti i documenti cartacei devono essere gestiti in modo da ridurre al minimo i tempi di permanenza al di fuori degli archivi o degli armadi o contenitori in dotazione alle unità operative. Massima attenzione dovrà essere posta per i documenti che si trovano in locali accessibili al pubblico. L'accesso agli archivi è consentito al personale a ciò espressamente autorizzato in via permanente od occasionale. Gli archivi devono essere mantenuti costantemente chiusi, compatibilmente con le esigenze di servizio. Le copie dei documenti vanno trattate, con riferimento alla tutela dei dati personali in esse contenuti, con la medesima diligenza riservata agli originali. Gli utenti sono tenuti a vigilare sull'accesso ai locali in cui operano da parte di personale non identificato o non autorizzato.

4. Collegamento ai sistemi da remoto (VPN)

Il Conservatorio di Musica "Arrigo Boito" si riserva di autorizzare, in relazione a motivate richieste, l'accesso da remoto ai propri sistemi informativi mediante canali di comunicazione protetti VPN (Virtual Private Network). Possono accedere da remoto all'infrastruttura IT tramite VPN solo gli utenti a cui sono

state consegnate le apposite credenziali di accesso personali, esclusivamente per il periodo di tempo necessario all'espletamento dei propri compiti, senza intralciare le normali operazioni di manutenzione preventiva dei sistemi (backup, controlli, …) operate dal Servizio ICT e previo rispetto del presente regolamento. Il Conservatorio di Musica "Arrigo Boito" può disattivare in qualsiasi momento le credenziali o disconnettere un accesso VPN, senza necessità di preventivo avviso, qualora la disattivazione sia necessaria all'integrità o al funzionamento dei propri servizi IT, oppure qualora vi sia fondato sospetto che l'Utente VPN abbia violato il presente Regolamento. Il Conservatorio di Musica "Arrigo Boito" potrà utilizzare sistemi di monitoraggio della rete e dei sistemi in grado di verificare che l'operato dell'Utente VPN risponda a quanto previsto dal presente Regolamento e nel rispetto delle normative vigenti

5. Collegamento alle reti wireless Istituzionali

Il collegamento alle reti wireless Istituzionali avviene secondo modalità e configurazioni di sicurezza prestabilite ed applicate dal Servizio ICT. L'utilizzo di tali tecnologie deve essere uniformato alle prescrizioni del presente regolamento. In particolare, è richiesto di:

- collegarsi alle reti wireless solamente mediante strumenti Istituzionali per fini lavorativi
- segnalare al Servizio ICT eventuali richieste di accesso alle reti wireless da parte di soggetti esterni (ospiti, consulenti, fornitori, ecc.).
- evitare l'utilizzo in autonomia e senza previa autorizzazione della Direzione e/o del Servizio ICT, di apparati che possano in qualche modo consentire l'accesso alla rete (ad esempio, Access Point WiFi, Router WIFi, …)

Art. 10 - Utilizzo della posta elettronica e dei sistemi di instant messaging/VoIP

1. L'abilitazione alla posta elettronica deve essere preceduta da regolare richiesta del responsabile di riferimento.
2. L'uso della casella di posta elettronica è fornito come strumento destinato esclusivamente all'utilizzo in ambito Istituzionale e per l'espletamento delle mansioni lavorative. Le persone assegnatarie delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse e devono utilizzare il form di firma così come approvato secondo gli standard del Conservatorio di Musica "Arrigo Boito".
3. L'uso di sistemi di Instant Messaging/VoIP è fornito come strumento destinato esclusivamente all'utilizzo in ambito Istituzionale e per l'espletamento delle mansioni lavorative.
4. È fatto divieto di utilizzare le caselle di posta elettronica Istituzionale per l'invio di messaggi personali o per la partecipazione a dibattiti, forum o mailing-list salvo diversa ed esplicita autorizzazione.
5. È altresì espressamente vietato utilizzare account diversi da quello Istituzionale per corrispondenza legata all'attività lavorativa in genere.
6. È buona norma evitare messaggi completamente estranei al rapporto di lavoro. La casella di posta deve essere mantenuta in ordine, cancellando documenti inutili e soprattutto allegati ingombranti.
7. Nel caso di mittenti sconosciuti o messaggi insoliti, per non correre il rischio di essere infettati da virus, occorrerà cancellare i messaggi senza aprirli.
8. È obbligatorio controllare i file allegati di posta elettronica prima del loro utilizzo.
9. In caso di ricezione di messaggi o files sospetti è necessario comunicare con il Servizio ICT per valutare come procedere.
10. Evitare che la diffusione incontrollata di 'catene di sant'Antonio' – messaggi a diffusione capillare e moltiplicata – limiti l'efficienza del sistema di posta
11. Utilizzare, nel caso di invio di allegati pesanti, i formati compressi (*.zip *.rsr *.jpg).
12. Nel caso in cui si debba inviare un documento all'esterno del Conservatorio di Musica "Arrigo Boito" è preferibile utilizzare un formato protetto da scrittura (ad esempio il formato Acrobat *.pdf).
13. Nel caso di assenza prevista e/o prevedibile il lavoratore, previa autorizzazione del proprio Responsabile, ha la facoltà di delegare un altro lavoratore "fiduciario" autorizzato a verificare il contenuto dei messaggi

indirizzati al collega delegante ed a inoltrare al datore di lavoro quelli del fiduciario ritenuti rilevanti per l'attività lavorativa. Il Servizio ICT si occuperà delle opportune configurazioni per permettere l'attivazione della delega. Per nessuna ragione il lavoratore delegante dovrà fornire le proprie Credenziali di Autenticazione al lavoratore delegato.

14. Risposta automatica: fuori ufficio. In caso di assenza programmata dall'ufficio deve essere attivato il messaggio di risposta automatica di non presenza in ufficio, senza rivelare il motivo dell'assenza e segnalando un sistema alternativo per permettere al corrispondente di sviluppare il contatto.

15. In base al principio della salvaguardia della continuità operativa del Conservatorio di Musica "Arrigo Boito", questa si riserva il diritto di accedere alle caselle di posta utilizzate dai dipendenti e collaboratori, nel caso si renda necessario utilizzare informazioni ivi contenute. A tal fine, l'accesso alle caselle dei dipendenti e collaboratori è consentito solo ai Responsabili di ogni reparto e al Responsabile del trattamento dei dati. In caso di accesso, il dipendente o collaboratore verrà informato dal Responsabile di Reparto e sarà obbligato a cambiare password al successivo accesso.

16. Non è consentito in ogni caso l'utilizzo della posta elettronica a dipendenti e collaboratori non autorizzati all'utilizzo degli strumenti informatici e telematici.

Art. 11 - Uso della rete internet e dei relativi servizi da PC/Notebook Istituzionale

1. L'uso dell'accesso alla rete Internet è fornito come strumento destinato esclusivamente all'utilizzo in ambito Istituzionale e per l'espletamento delle mansioni lavorative.
2. È assolutamente proibita la navigazione in Internet per motivi diversi da quelli strettamente legati all'attività lavorativa stessa,
3. È fatto divieto all'utente lo scarico di software gratuito (freeware e shareware) prelevato da siti Internet, se non espressamente e preventivamente autorizzato dal Servizio ICT.
4. È tassativamente vietata l'effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti on-line e simili salvo i casi direttamente autorizzati dalla Direzione e con il rispetto delle normali procedure già in uso per l'attività tradizionale.
5. È da evitare ogni forma di registrazione a siti i cui contenuti non siano legati all'attività lavorativa.
6. È vietata la partecipazione a forum non professionali, l'utilizzo di chat-line e l'utilizzo di bacheche elettroniche anche utilizzando pseudonimi.
7. Al fine di evitare usi impropri della navigazione in Internet, la Direzione Istituzionale si riserva di utilizzare appositi software allo scopo di prevenire le suddette operazioni vietate in quanto non inerenti agli scopi dell'attività lavorativa (filtri, particolari configurazioni di sistema).
8. Non è consentito in ogni caso l'utilizzo di internet ai dipendenti non autorizzati all'utilizzo degli strumenti informatici e telematici.

Art. 12 - Protezione antivirus

1. Ogni utente deve tenere comportamenti tali da ridurre il rischio di attacco al Sistema Informatico Istituzionale mediante virus o mediante ogni altro software a rischio.
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) e segnalare l'accaduto al Servizio ICT.
3. Non è consentito l'utilizzo di supporto magnetici e/o ottici di provenienza ignota.

Art. 13 - Osservanza delle disposizioni in materia di Privacy

1. E' obbligatorio attenersi alle disposizioni in materia di privacy e di misure minime di sicurezza, come indicate nella lettera di individuazione dell'autorizzato del trattamento dei dati.

Art. 14 - Non osservanza della normativa Istituzionale

1. Il mancato rispetto o la violazione dei contenuti del presente regolamento è perseguibile, secondo quanto previsto dai contenuti della Disciplina Generale sez. Terza (Disciplina Comune del Rapporto Individuale di Lavoro) del vigente C.C.N.L. applicato dal Conservatorio di Musica "Arrigo Boito", con provvedimenti disciplinari nonché con le azioni civili e penali consentite.

Art. 15 - Controlli

1. La Direzione Istituzionale si riserva la facoltà di effettuare controlli per verificare l'integrità del sistema informatico e per l'ordinaria manutenzione dello stesso.
2. In tale sede provvederà ad accertare e segnalare tempestivamente eventuali abusi commessi dal lavoratore.
3. Potranno essere effettuati controlli in base al principio della salvaguardia e della continuità operativa del *Conservatorio di Musica "Arrigo Boito"*.
4. Gli eventuali monitoraggi saranno condotti nel modo meno invasivo possibile, avuto riguardo all'interesse tutelato, ai rischi che si intendono evitare ed alle finalità perseguite.
5. I dati personali eventualmente raccolti in occasione dei controlli non saranno utilizzati per fini estranei o per un tempo superiore a quanto strettamente necessario all'eventuale procedimento disciplinare o agli accertamenti su violazioni di terzi.
6. Tali controlli avverranno nel pieno rispetto della privacy dei lavoratori e delle regole Istituzionali previste per il trattamento dei dati personali e avuto riguardo ai controlli espressamente vietati dal Garante nel provvedimento deliberato in data 1 marzo 2007.

Art. 16 - Aggiornamenti e revisioni

1. Tutti gli utenti possono proporre, quando ritenuto necessario, integrazioni al presente Regolamento.
2. Le proposte verranno esaminate dalla Direzione.
3. Il presente Regolamento potrà essere soggetto a revisioni periodiche.

APPENDICE 1: NORMATIVE APPLICABILI

CODICE PRIVACY E PROVVEDIMENTI GARANTE:

- Regolamento UE 679/2016 e D.Lgs. 196/2003 e s.m.i. (D. Lgs. 101/2018).
- Provvedimento del Garante Privacy del 1 marzo 2007 *(G.U. n° 58 del 10/3/2007) "Lavoro: le linee guida del Garante per posta elettronica e internet"*
- Provvedimento del Garante Privacy del 27 novembre 2008 *(G.U. n. 300 del 24/12/ 2008) "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema"*
- Delibera del Garante Privacy N° 53 del 23 novembre 2006 *"Linee guida in materia di trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro alle dipendenze di datori di lavoro privati"*

STATUTO DEI LAVORATORI

- Art. 4 L.300/70, così come modificato dall'Art.23 del D. Lgs.151/2015 (c.d. Jobs Act) di seguito integralmente riportato:
  Modifiche all'articolo 4 della legge 20 maggio 1970, n. 300 e all'articolo 171 del decreto legislativo 30 giugno 2003, n.
  196
  1. L'articolo 4 della legge 20 maggio 1970, n. 300 è sostituito dal seguente:
  «Art. 4 (Impianti audiovisivi e altri strumenti di controllo).

1. *Gli impianti audiovisivi e gli altri strumenti dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori possono essere impiegati esclusivamente per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio Istituzionale e possono essere installati previo accordo collettivo stipulato dalla rappresentanza sindacale unitaria o dalle rappresentanze sindacali Istituzionali. In alternativa, nel caso di imprese con unità produttive ubicate in diverse province della stessa regione ovvero in più regioni, tale accordo può essere stipulato dalle associazioni sindacali comparativamente più rappresentative sul piano nazionale. In mancanza di accordo gli impianti e gli strumenti di cui al periodo precedente possono essere installati previa autorizzazione della Direzione territoriale del lavoro o, in alternativa, nel caso di imprese con unità produttive dislocate negli ambiti di competenza di più Direzioni territoriali del lavoro, del Ministero del lavoro e delle politiche sociali.*
2. *La disposizione di cui al comma 1 non si applica agli strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa e agli strumenti di registrazione degli accessi e delle presenze.*
3. *Le informazioni raccolte ai sensi dei commi 1 e 2 sono utilizzabili a tutti i fini connessi al rapporto di lavoro a condizione che sia data al lavoratore adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli e nel rispetto di quanto disposto dal decreto legislativo 30 giugno 2003, n. 196.».*

REATI INFORMATICI ED ALTRE VIOLAZIONI PENALMENTE SANZIONABILI

- Codice Penale: Art. 594 (Ingiuria), 595 (Diffamazione), 615 ter (Accesso abusivo ad un sistema informatico o telematico), 615 quater (Detenzione e diffusione abusiva di codici di accesso a sistemi informatici e telematici), 615 quinques (Diffusione di programmi diretti a danneggiare o interrompere un sistema informatico), 616 (Violazione, sottrazione e soppressione di corrispondenza), 640 ter (Frode informatica)

DIRITTO D'AUTORE

- L.633/1941 e D.Lgs. 518/1992 (Protezione del diritto d'autore e di altri diritti connessi al suo esercizio);

TUTELA INFORMAZIONI RISERVATE

- Art. 2105 e 2106 del Codice Civile ed Art. 98 e 99 del Codice della Proprietà Industriale (norme relative alle informazioni coperte da segreto)

APPENDICE 2: INFORMATIVA SUL TRATTAMENTO DEI DATI

Il presente regolamento è da considerarsi parte integrante dell'informativa fornita al personale interno (Regolamento UE 679/2016 e D.Lgs. 196/2003 e s.m.i. – D.Lgs. 101/2018) con specifico riferimento al trattamento di dati personali dei lavoratori stoccati nelle infrastrutture di rete, negli strumenti elettronici assegnati, negli apparati audiovisivi Istituzionali. A completamento delle informazioni contenute nel presente Regolamento si segnala:

Finalità e modalità del trattamento: i dati vengono memorizzati dalle infrastrutture tecnologiche per esigenze organizzative / produttive / tutela del patrimonio Istituzionale, per finalità principalmente connesse alla sicurezza e controllo costi.

Conferimento dati: i dati vengono registrati in modo automatico dagli strumenti tecnologici, pertanto non sono oggetto di conferimento da parte dell'utente. Tutti i dati vengono archiviati nell'infrastruttura informatica del *Conservatorio di Musica "Arrigo Boito"* e conservati per tempi compatibili con le finalità di sicurezza ed eventuale esercizio del diritto di difesa in sede giudiziaria. Specifiche misure di sicurezza sono osservate per prevenire la perdita dei dati, usi illeciti o non corretti ed accessi non autorizzati.

Ambito di comunicazione: i dati potranno essere trattati esclusivamente da personale appositamente nominato incaricato del trattamento ed amministratore di sistema. I dati non saranno oggetto di comunicazione o diffusione, ad eccezione di specifiche richieste di accesso da parte delle forze dell'ordine ed autorità giudiziaria. Gli utenti possono richiedere in qualsiasi momento gli estremi identificativi.

Durata del trattamento: la conservazione dei dati avverrà per il periodo necessario al raggiungimento dello scopo per cui gli stessi sono stati raccolti.

Diritti degli interessati: i soggetti cui si riferiscono i dati personali hanno il diritto in qualunque momento di ottenere la conferma dell'esistenza o meno dei medesimi dati e di conoscerne il contenuto e l'origine, verificarne l'esattezza o chiederne l'integrazione o l'aggiornamento, oppure la rettificazione (articolo 7 del Codice in materia di protezione dei dati personali). Ai sensi del medesimo articolo si ha il diritto di chiedere la cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge, nonché di opporsi in ogni caso, per motivi legittimi, al loro trattamento.