



Ministero dell'Istruzione, dell'Università e della Ricerca  
*Alta Formazione Artistica Musicale e Coreutica*  
**Conservatorio di Musica "Giacomo PUCCINI"**  
Istituzione di Alta Cultura

Via XX Settembre, 34 19121 – LA SPEZIA  
Tel. 0187/77.03.33 - Fax 0187/77.03.41 – email: [info@conservatoriopuccini.com](mailto:info@conservatoriopuccini.com)

Docente M° \_\_\_\_\_

**Oggetto: Lettera di nomina quale persona autorizzata al trattamento dati**

Il Conservatorio "G.Puccini" della Spezia, in qualità di Titolare del trattamento dei dati, **conferisce** alla Sig./Sig.ra \_\_\_\_\_, Nato a \_\_\_\_\_ il \_\_\_\_\_, Docente di \_\_\_\_\_, l'**incarico** di compiere le operazioni di trattamento di seguito elencate, con l'avvertimento che dovrà operare osservando le direttive del Titolare.

Operazioni:

- Attività didattica e tutti adempimenti ad essa connessi previsti dal proprio ruolo nell'Istituto secondo quanto autorizzato dal proprio contratto di lavoro in essere e da specifici incarichi assegnati dalla Direzione;
  - Partecipazione agli organi collegiali istituiti nel Conservatorio come da Statuto e Regolamenti interni;
  - Attività artistica e di produzione connessa ai Progetti realizzati dal Conservatorio;
- I dati oggetto del trattamento, connessi alle predette finalità, sono quelli relativi a studenti e docenti del Conservatorio e riferiti a dati COMUNI nello specifico Nome Cognome, Dati anagrafici, Codice Fiscale, Email, Recapito telefonico

A tal fine, vengono fornite informazioni ed istruzioni per l'assolvimento del compito assegnato:

- il trattamento dei dati deve essere effettuato in modo lecito e corretto;
- i dati personali devono essere raccolti e registrati unicamente per finalità inerenti l'attività svolta;
- è necessaria la verifica costante dei dati ed il loro aggiornamento;
- è necessaria la verifica costante della completezza e pertinenza dei dati trattati;
- devono essere rispettate le misure di sicurezza predisposte dal Titolare;
- in ogni operazione del trattamento deve essere garantita la massima riservatezza ed in particolare:
  - a) divieto di comunicazione e/o diffusione dei dati senza la preventiva autorizzazione del Titolare;
  - b) l'accesso ai dati dovrà essere limitato all'espletamento delle proprie mansioni ed esclusivamente negli orari di lavoro;
  - c) la fase di raccolta del consenso dovrà essere preceduta dalla informativa ed il consenso al trattamento degli interessati rilasciato in forma scritta;
- in caso di interruzione, anche temporanea, del lavoro verificare che i dati trattati non siano accessibili a terzi non autorizzati;
- le proprie credenziali di autenticazione devono essere riservate;
- svolgere le attività previste dai trattamenti secondo le direttive del Titolare del trattamento dei dati; non modificare i trattamenti esistenti o introdurre nuovi trattamenti senza l'esplicita autorizzazione del Titolare del trattamento dei dati;
- rispettare e far rispettare le norme di sicurezza per la protezione dei dati personali;
- informare il Titolare del trattamento dei dati in caso di incidente di sicurezza che coinvolga dati particolari e non;
- raccogliere, registrare e conservare i dati presenti negli atti e documenti contenuti nei fascicoli di studio e nei supporti informatici avendo cura che l'accesso ad essi sia possibile solo ai soggetti autorizzati;
- eseguire qualsiasi altra operazione di trattamento nei limiti delle proprie mansioni e nel rispetto delle norme di legge;
- qualsiasi altra informazione può essere fornita dal Titolare che provvede anche alla formazione.

Gli obblighi relativi alla riservatezza, alla comunicazione ed alla diffusione dovranno essere osservati anche in seguito a modifica dell'incarico e/o cessazione del rapporto di lavoro.

Si allegano alla presente più dettagliate istruzioni e regole operative in caso di violazione del dato.

Per conoscenza ed accettazione Persona autorizzata al trattamento dati (NOME COGNOME)  _____ (firma)	Il Titolare del trattamento  _____ (firma)
---	---

## ISTRUZIONE OPERATIVA DATA BREACH

L'art. 33 del **Regolamento Europeo 679/2016 (GDPR)** impone al titolare del trattamento di notificare all'autorità di controllo la violazione di dati personali (**data breach**) entro 72 ore dal momento in cui ne viene a conoscenza.

L'obbligo di notifica scatta se la violazione, ragionevolmente, comporta un rischio per i diritti e le libertà delle persone fisiche, qualora, poi, il rischio fosse elevato, allora, oltre alla notifica, il titolare è tenuto a darne comunicazione all'interessato.

Il termine per adempiere alla notifica è brevissimo, 72 ore dal momento in cui il titolare ne viene a conoscenza, mentre, l'eventuale comunicazione agli interessati, deve essere fatta senza indugio.

L'eventuale ritardo nella notificazione deve essere giustificato, il mancato rispetto dell'obbligo di notifica, invece, pone l'autorità di controllo nella condizione di applicare le misure correttive a sua disposizione ovvero: l'esercizio dei poteri previsti dall'art.58 GDPR (avvertimenti, ammonimenti, ingiunzioni, imposizione di limiti al trattamento, ordine di rettifica, revoca di certificazioni, ordine di sospendere flussi dati), la imposizione di sanzioni amministrative secondo l'art. 83 GDPR.

Per "**Violazione di dati**" si intende la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati (Art. 4 p.12 del GDPR).

La violazione di dati è un particolare tipo di incidente di sicurezza, per effetto del quale, il titolare non è in grado di garantire il rispetto dei principi prescritti dall'art. 5 del GDPR per il trattamento dei dati personali.

Preliminarmente, dunque, il titolare deve poter identificare l'incidente di sicurezza in genere, quindi, comprendere che l'incidente ha impatto sulle informazioni e, infine, che tra le informazioni coinvolte dall'incidente vi sono dati personali.

L'art. 33 p.5 del GDPR prescrive al titolare di documentare qualsiasi violazione dei dati personali, al fine di consentire all'autorità di controllo di verificare il rispetto della norma.

L'art. 33 p.2 GDPR prevede espressamente il dovere per il responsabile, quando viene a conoscenza di una violazione, di informare, senza ingiustificato ritardo, il titolare.

E' importante che sia dimostrabile il momento della scoperta dell'incidente, poiché da quel momento decorrono le 72 ore per la notifica.

Si possono distinguere tre tipi di violazioni:

violazione di riservatezza, ovvero quando si verifica una divulgazione o un accesso a dati personali non autorizzato o accidentale;

violazione di integrità, ovvero quando si verifica un'alterazione di dati personali non autorizzata o accidentale;

violazione di disponibilità, ovvero quando si verifica perdita, inaccessibilità, o distruzione, accidentale o non autorizzata, di dati personali.

Una violazione potrebbe comprendere una o più tipologie.

Per comprendere quando notificare la violazione è opportuno effettuare una valutazione dell'entità dei rischi:

- **Rischio assente:** la notifica al Garante non è obbligatoria.
- **Rischio presente:** è necessaria la notifica al Garante.
- **Rischio elevato:** In presenza di rischi "elevati", è necessaria la comunicazione agli interessati. Nel momento in cui il titolare del trattamento adotta sistemi di crittografia dei dati, e la violazione non comporta l'acquisizione della chiave di decrittografia, la comunicazione ai soggetti interessati non sarà un obbligo.

I rischi per i diritti e le libertà degli interessati possono essere considerati "elevati" quando la violazione può, a titolo di esempio:

- b. coinvolgere un rilevante quantitativo di dati personali e/o di soggetti interessati;
- c. riguardare categorie particolari di dati personali;
- d. comprendere dati che possono accrescere ulteriormente i potenziali rischi (es. dati di localizzazione, finanziari, relativi alle abitudini e preferenze);
- e. comportare rischi imminenti e con un'elevata probabilità di accadimento (es. rischio di perdita finanziaria in caso di furto di dati relativi a carte di credito);
- f. impattare su soggetti che possono essere considerati vulnerabili per le loro condizioni (es. pazienti, minori, soggetti indagati).

Per la notifica della violazione e la comunicazione al Garante occorre compilare gli appositi moduli messi a disposizione.

### **Nota Bene:**

**Nel caso in cui Lei venisse a conoscenza di un ipotesi di violazione del dato sarà tenuta a comunicare immediatamente la notizia al Titolare (nella persona del Presidente del Conservatorio *pro tempore*).**

Data .....

Firma ricevuta istruzione .....

# ISTRUZIONI OPERATIVE INCARICATI DEL TRATTAMENTO

## Indice

### Premessa

- Definizioni
- Adempimenti
- Modalità di svolgimento delle operazioni
- Istruzioni per l'uso degli strumenti informatici
  - Gestione strumenti elettronici (pc fissi e portatili)
  - Gestione username e password
  - Installazione di hardware e software
  - Gestione posta elettronica del Conservatorio G Puccini.
  - Gestione del salvataggio dei dati
  - Gestione dei supporti rimovibili
  - Gestione protezione dai virus informatici
  - Uso della rete internet e dei relativi servizi
  - Telefonia mobile
- Istruzioni per l'uso degli strumenti "non elettronici"
  - distruzione delle copie cartacee
  - Misure di sicurezza
  - Prescrizioni per gli incaricati
- Addetti alla manutenzione
- Osservanza delle disposizioni in materia di Privacy.
- Non osservanza della normativa del Conservatorio G Puccini.
- Aggiornamento e revisione

### PREMESSA

Il presente documento contiene le istruzioni operative per gli Incaricati del trattamento dei dati personali del Conservatorio G Puccini conformemente al Regolamento (Ue) 2016/679 (GDPR). I dipendenti, i collaboratori, i consulenti, i volontari ed in generale tutte le persone autorizzate ad accedere ai dati personali e preposte allo svolgimento delle operazioni di trattamento relativa ai dati, devono ispirarsi a un principio generale di diligenza e correttezza. Ogni utilizzo dei dati in possesso del Conservatorio G Puccini diverso da finalità strettamente professionali, è espressamente vietato. Di seguito vengono esposte le regole comportamentali da seguire per evitare e prevenire condotte che anche inconsapevolmente potrebbero comportare rischi alla sicurezza del sistema informativo e all'immagine del Conservatorio G Puccini.

### DEFINIZIONI

Secondo l'articolo 4 del Regolamento (Ue) 2016/679 (GDPR), si definisce:

**Dato personale:** qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;

**Trattamento:** qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;

**Violazione dei dati personali:** la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.

### ADEMPIMENTI

Ciascun incaricato del trattamento deve:

- g. rispettare i principi generali del Regolamento (Ue) 2016/679 (GDPR), con particolare riferimento alla liceità e correttezza del proprio agire, all'obbligo di procedere alla raccolta e alla registrazione dei dati per scopi determinati, espliciti e legittimi;
- h. rispettare l'obbligo di riservatezza e segretezza e conseguentemente il divieto di comunicazione e diffusione dei dati trattati nel corso dell'incarico svolto;
- i. utilizzare i dati, cui abbia accesso, solamente per finalità compatibili all'esecuzione delle proprie mansioni o dei compiti affidati, per cui è autorizzato ad accedere alle informazioni e ad utilizzare gli strumenti del Conservatorio G Puccini;
- j. rispettare le misure di sicurezza idonee adottate dalla società, atte a salvaguardare la riservatezza e l'integrità dei dati;
- k. segnalare eventuali malfunzionamenti di strumenti elettronici, perdite di dati o esigenze (sia di natura organizzativa, sia tecnica), che possano migliorare lo svolgimento delle operazioni affidate;
- l. accedere ai dati strettamente necessari all'esercizio delle proprie funzioni e competenze;
- m. in caso di interruzione del lavoro, anche temporanea, verificare che i dati trattati non siano accessibili a terzi non autorizzati;
- n. mantenere riservate le proprie credenziali di autenticazione;
- o. svolgere le attività previste dai trattamenti secondo le direttive del responsabile del trattamento dei dati; non modificare i trattamenti esistenti o introdurre nuovi trattamenti senza l'esplicita autorizzazione del responsabile del trattamento dei dati;
- p. rispettare e far rispettare le norme di sicurezza per la protezione dei dati personali;
- q. informare il responsabile in caso di incidente di sicurezza che coinvolga dati particolari e non;
- r. raccogliere, registrare e conservare i dati presenti negli atti e documenti contenuti nei fascicoli dello Conservatorio G Puccini e nei supporti informatici avendo cura che l'accesso ad essi sia possibile solo ai soggetti autorizzati;
- s. eseguire qualsiasi altra operazione di trattamento nei limiti delle proprie mansioni e nel rispetto delle norme di legge.

## MODALITÀ DI SVOLGIMENTO DELLE OPERAZIONI

Le principali operazioni degli incaricati del trattamento sono:

- identificazione dell'interessato:

al momento della raccolta dei dati personali, qualora sia necessario individuare l'identità del soggetto che fornisce le informazioni, è obbligatorio richiedere un documento di identità o di riconoscimento, al fine di verificare la identità e di procedere correttamente alla raccolta e alla registrazione delle informazioni;

- verifica del controllo dell'esattezza del dato e della corretta digitazione:

al momento della registrazione dei dati raccolti, occorre prestare attenzione alla digitazione e all'inserimento dei dati identificativi e degli altri dati riferiti all'interessato, al fine di evitare errori, che potrebbero generare problemi nella corretta gestione dell'anagrafica e nello svolgimento delle operazioni, che caratterizzano il processo di trattamento;

- Norme logistiche per l'accesso fisico ai locali:

I locali, ove sono custoditi i dati personali (ed in special modo quelli definiti particolari dal Regolamento cc.dd. ex sensibili), devono essere soggetti a controllo e a verifica, al fine di evitare che durante l'orario di lavoro possano essere conosciuti o accessibili da parte di soggetti non autorizzati. Si raccomanda, in caso di allontanamento dal proprio ufficio o dalla propria postazione di lavoro, di adottare tutte le accortezze e precauzioni al fine di impedire l'accesso fisico a chi non sia legittimato, soprattutto se esterno all'organizzazione di appartenenza. Laddove si esegue il trattamento di Dati Personali, deve essere possibile ricoverare in luogo sicuro i documenti cartacei ed i supporti rimovibili contenenti tali dati. Pertanto le porte degli uffici ed almeno un armadio per ufficio devono essere dotati di serratura con chiave. Al termine dell'orario lavorativo, ove la dinamica delle attività ed il numero di occupanti lo consentano, è necessario chiudere sempre a chiave gli uffici nei quali vengono svolti trattamenti di Dati Personali.

- Dati Particolari

Il Regolamento 2016/679 definisce all'art. 9 i dati particolari come quei dati capaci di rivelare l'origine razziale o etnica dell'interessato, le sue opinioni politiche, le convinzioni religiose o filosofiche o l'appartenenza sindacale, nonché i dati genetici, i dati biometrici intesi ad identificare in modo univoco una persona fisica, i dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.

Il trattamento dei dati particolari dovrà avvenire nel rispetto del Regolamento, provvedendo a separare tali dati dai dati comuni all'interno degli archivi mediante una cartellina fisica e/o informatica apposita che dovrà essere visibile soltanto agli incaricati appositamente autorizzati; impedendo a terzi non autorizzati l'accesso a tali dati; utilizzando buste chiuse per contenuti particolari sulla salute che dovranno essere consegnate al titolare per i relativi obblighi di legge.

### ISTRUZIONI PER L'USO DEGLI STRUMENTI INFORMATICI

Come principio generale, sia i dispositivi di memorizzazione del proprio PC sia le unità di rete, devono contenere informazioni strettamente professionali e non possono essere utilizzate per scopi diversi (immagini, video e documenti personali).

Di seguito sono riportate le indicazioni per la gestione dei diversi strumenti informatici per il trattamento dati:

#### a) Gestione strumenti elettronici (pc fissi e portatili)

Ciascun incaricato è responsabile del corretto utilizzo e della custodia degli strumenti elettronici in dotazione (a titolo esemplificativo personal computer, periferiche, lettori di smart card). Si devono adottare le misure di sicurezza per la tutela della riservatezza, consistenti nell'evitare che l'accesso ai dati possa avvenire da parte di soggetti estranei all'organizzazione o non specificamente autorizzati. Al fine di verificare il corretto utilizzo degli strumenti in dotazione potranno essere svolti controlli a campione mediante la raccolta e l'analisi di dati aggregati e anonimi. Inoltre, nel caso di provato o constatato uso illecito o non consentito degli strumenti elettronici, risultante dalla verifica delle informazioni in modalità aggregata e anonima, può essere necessario procedere alla verifica delle registrazioni delle sessioni di lavoro, al fine di sanzionare condotte illecite, anche su richiesta dell'autorità giudiziaria, cui le informazioni potranno essere comunicate, senza alcuna ulteriore informativa all'interessato.

Il Personal Computer affidato al dipendente è uno **strumento di lavoro**. Ogni utilizzo non inerente all'attività lavorativa può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza.

L'accesso all'elaboratore è protetto da password che deve essere custodita dall'incaricato con la massima diligenza e non divulgata.

E' nominato dal Conservatorio G Puccini un custode delle parole chiave riservate che potrà accedere ai dati ed agli strumenti informatici esclusivamente per permettere allo Conservatorio G Puccini, Titolare del trattamento, di accedere ai dati trattati da ogni incaricato – secondo specifiche modalità - al solo fine di garantire l'operatività, la sicurezza del sistema ed il normale svolgimento dell'attività di lavoro nei casi in cui si renda indispensabile ed indifferibile l'intervento, ad esempio, in caso di prolungata assenza o impedimento dell'incaricato, informando tempestivamente l'incaricato dell'intervento di accesso realizzato.

Saranno messe a disposizione di ciascun lavoratore apposite funzionalità di sistema che consentano di inviare automaticamente, in caso di assenza prolungate, messaggi di risposta che contengano le coordinate di altro soggetto o altre utili modalità di contatto dell'Ufficio presso la quale il lavoratore assente opera. In caso di assenza improvvisa e prolungata e per improrogabili necessità legate all'attività lavorativa, l'interessato dovrà delegare un altro lavoratore (fiduciario) a verificare il contenuto dei messaggi e ad inoltrare al titolare del trattamento quelli ritenuti rilevanti per lo svolgimento dell'attività lavorativa. Di tale attività sarà redatto apposito verbale e informato il lavoratore interessato alla prima occasione utile.

Per la gestione della sessione di lavoro sul pc (fisso e portatile), è necessario che:

- al termine delle ore di servizio, il PC deve essere spento, a meno che non stia svolgendo elaborazioni particolari. In tal caso gli uffici debbono tassativamente essere chiusi a chiave;
- Se l'incaricato si assenta momentaneamente dalla propria postazione deve accertarsi che l'eventuale sessione di lavoro aperta non sia accessibile da altre persone. Pertanto deve chiudere la sessione di lavoro sul PC facendo Logout, oppure in alternativa deve avere attivo un salvaschermo (screen- saver) protetto dalle credenziali di autenticazione;
- Relativamente all'utilizzo dello screen-saver, occorre osservare le seguenti norme:
  - Non deve mai essere disattivato;
  - Il suo avvio automatico deve essere previsto non oltre i primi 10 minuti di inattività del PC;
  - Deve essere messo in funzione manualmente ogni volta che si lascia il PC incustodito ed acceso;
- Quando si esegue la stampa di un documento contenente dati personali, in particolare su una stampante condivisa, occorre ritirare tempestivamente i documenti stampati per evitare l'accesso a soggetti non abilitati al trattamento.

Per l'utilizzo dei PC portatili valgono le regole elencate per i PC connessi alla rete, con le seguenti ulteriori raccomandazioni:

- prima della riconsegna, rimuovere eventuali file ivi elaborati;
- quando il PC portatile è nei locali del Conservatorio G Puccini, non lasciarlo mai incustodito; in caso di brevi assenze assicurarne alla scrivania o ad elementi "sicuri" dell'arredamento (maniglie, intelaiature...) utilizzando gli appositi cavi in acciaio dotati di lucchetto;
- quando il PC portatile è all'esterno del Conservatorio G Puccini, evitare di lasciarlo incustodito;
- per assenze prolungate, anche qualora l'ambiente venga ritenuto "affidabile", è necessario custodire il portatile in modo opportuno es. cassaforte;
- in caso di furto di un portatile è necessario avvertire tempestivamente il responsabile del Servizio Informatico, onde prevenire possibili intrusioni ai sistemi del Conservatorio G Puccini;
- in caso di viaggio aereo trasportare tassativamente il portatile come bagaglio a mano;
- eseguire periodicamente salvataggi dei dati e non tenere tali backup insieme al PC portatile.

#### **b) Gestione username e password**

L'accesso al PC, sia esso collegato in rete o meno, è protetto da un sistema di autenticazione che richiede all'Incaricato di inserire sulla videata di accesso all'elaboratore un codice utente (username) ed una parola chiave (password). L'adozione ed il corretto utilizzo della combinazione username / password è fondamentale per il corretto utilizzo del PC, in quanto:

- tutela l'utilizzatore ed in generale il Conservatorio G Puccini da accessi illeciti, atti di vandalismo e, in generale, violazioni e danneggiamenti del proprio patrimonio informativo;
- tutela l'Incaricato da false imputazioni, garantendo che nessuno possa operare a suo nome e che, con il suo profilo (ossia con le sue user id e password) solo lui possa svolgere determinate azioni;
- è necessario per gestire correttamente gli accessi a risorse condivise.

Ciascun incaricato deve scegliere le password in base ai seguenti criteri:

- devono essere lunghe almeno otto caratteri;
- non devono fare riferimento ad informazioni agevolmente riconducibili ai soggetti utilizzatori o ai loro famigliari;
- devono contenere una combinazione di numeri e/o segni speciali, lettere, maiuscole e minuscole;
- non deve essere uguale alle precedenti.

Per la corretta gestione della password è necessario:

- Almeno ogni 2 mesi è obbligatorio cambiare la password;
- Ogni password ricevuta va modificata al primo utilizzo;
- La password venga conservata in un luogo sicuro;
- Non rivelare o condividere la password con i colleghi di lavoro, famigliari e amici, soprattutto attraverso il telefono;
- Non utilizzare la funzione, offerta da alcuni software, di salvare automaticamente la password per successivi utilizzi delle applicazioni.

#### **c) Installazione di hardware e software**

L'installazione di hardware e software, nonché la modifica dei parametri di configurazione, possono essere eseguiti solamente dalle persone del Servizio Informatico su mandato del Titolare. Pertanto si raccomanda agli utenti dei PC di rispettare i seguenti divieti:

- Non utilizzare sul PC dispositivi personali, o comunque non dello Conservatorio G Puccini, quali lettori dispositivi di memorizzazione dei dati;
- Non installare sistemi per connessione esterne (es : modem, wifi); tali connessioni, aggirando i sistemi preposti alla sicurezza della rete dello Conservatorio G Puccini, aumentano sensibilmente i rischi di intrusioni e di attacchi dall'esterno;
- Non installare programmi, anche in versione demo. In particolare, è vietata l'installazione di giochi, programmi in prova (shareware), programmi gratuiti (freeware), programmi pirata, e in generale tutti i software non autorizzati dal Servizio Informatico;
- Non modificare i parametri di configurazione del proprio PC senza espressa autorizzazione e senza il supporto di personale tecnico qualificato.

Si ricorda che normalmente la condivisione di aree e di risorse del proprio PC è vietata. Può essere autorizzata dal Servizio Informatico, solo in casi eccezionali e solo per il tempo strettamente necessario allo svolgimento delle attività di lavoro. In questi casi devono essere adottate password di lettura e scrittura e la condivisione deve operare solo su singole directory del PC, e non sull'intero disco rigido.

#### **d) Gestione posta elettronica del Conservatorio G Puccini**

Il servizio di posta elettronica viene fornito per permettere la comunicazione con soggetti terzi interni ed esterni per le finalità del Conservatorio G Puccini e in stretta connessione con l'effettiva attività e mansioni del lavoratore o del volontario che utilizza tale funzionalità.

Al fine di non compromettere la sicurezza del Conservatorio G Puccini e di prevenire conseguenze legali a carico della stessa, bisogna adottare le seguenti norme comportamentali:

- Se si ricevono mail da destinatari sconosciuti contenenti file di qualsiasi tipo, procedere alla loro immediata eliminazione;
- È fatto divieto di utilizzare le caselle di posta elettronica per l'invio di messaggi personali o per la partecipazione a dibattiti, forum o mail list, salvo diversa ed esplicita autorizzazione; a tal fine nel messaggio dovrà essere contenuta l'indicazione della natura non personale della comunicazione e deve essere specificato che le risposte potranno essere conosciute nell'Organizzazione del mittente;
- La casella di posta elettronica assegnata deve essere mantenuta in ordine, cancellando i documenti inutili specialmente se contengono allegati ingombranti come dimensione.

Nell'ipotesi in cui la email debba essere utilizzata per la trasmissione di dati particolari (ex dati sensibili), si raccomanda di prestare attenzione a che:

- l'indirizzo del destinatario sia stato correttamente digitato,
- l'oggetto del messaggio non contenga direttamente il riferimento a stati, fatti o qualità idonei a rivelare dati di natura sensibile;
- nel corpo del messaggio sia presente un'intestazione standardizzata in cui si avverta della confidenzialità/riservatezza del messaggio.

In caso di errore nella spedizione o ricezione, contattare rispettivamente il destinatario cui è stata trasmessa per errore la comunicazione o il mittente che, per errore, l'ha spedita, eliminando quanto ricevuto (compresi allegati) senza effettuare copia.

#### **e) Gestione del salvataggio dei dati**

Per i dati ed i documenti che risiedono sui server gestiti centralmente, come ad esempio cartelle di rete e database, il Servizio Informatico esegue i salvataggi con la possibilità di ripristinare in toto oppure selettivamente eventuali files distrutti, ad esempio per guasti hardware oppure per cancellazioni involontarie.

Per i dati ed i documenti che risiedono esclusivamente sul PC, ogni Incaricato deve eseguire almeno una volta alla settimana la copia (salvataggio, o backup). Questo allo scopo di garantire la disponibilità ed il ripristino dei Dati Personali nel caso di una generica compromissione delle risorse (cancellazioni accidentali, guasti, furti...). L'Incaricato deve verificare che i supporti informatici utilizzati per il backup, che normalmente sono dischi magnetici esterni, CD, DVD oppure flash disks (chiavette) siano funzionali e non corrotti.

#### **f) Gestione dei supporti rimovibili**

I supporti rimovibili, come ad esempio dischi magnetici esterni, penne USB o CD riscrivibili, quando contengono dati personali devono essere custoditi in luogo protetto e non accessibile (cassaforte, armadio chiuso a chiave, etc.). Quando non sono più utilizzati devono essere distrutti o resi inutilizzabili, ovvero possono essere riutilizzati da altri Incaricati non autorizzati al trattamento degli stessi dati, soltanto dopo essere stati formattati. Tali operazioni vengono effettuate a cura del servizio Sistemi. Il trasferimento di file contenenti dati personali, dati particolari (ex dati sensibili) e giudiziari su supporti rimovibili, è da eseguire unicamente in via transitoria, ponendo la massima attenzione alla destinazione di trasferimento e cancellando i file appena possibile. I dati particolari (ex dati sensibili) e giudiziari devono essere crittografati.

#### **g) Gestione protezione dai virus informatici**

Per prevenire eventuali danneggiamenti al software causati dalla presenza o dall'azione di programmi virus informatici, su ogni elaboratore del Conservatorio G Puccini è stato installato un software antivirus che si aggiorna automaticamente all'ultima versione disponibile.

L'antivirus non deve mai essere disattivato o sostituito con altro antivirus non ufficialmente fornito.

Nel caso il programma antivirus installato sul proprio PC riscontri la presenza di un virus, oppure si sospetti la presenza di un virus non rilevato dal programma antivirus è necessario darne immediatamente segnalazione al responsabile del Servizio Informatico.

Si raccomanda di non scaricare e né tantomeno aprire file provenienti via e-mail da mittenti sconosciuti. Tali file, possono essere

portatori di virus e compromettere la funzionalità del PC, l'integrità dei dati in essa contenuti e soprattutto l'integrità dei sistemi collegati al PC stesso.

#### **h) Uso della rete internet e dei relativi servizi**

Il PC abilitato alla navigazione in Internet costituisce uno strumento del Conservatorio G Puccini necessario allo svolgimento della propria attività lavorativa. È assolutamente proibita la navigazione in Internet per motivi diversi da quelli strettamente legati all'attività lavorativa stessa.

È fatto divieto all'utente lo scarico di software gratuito (freeware) e shareware prelevato da siti Internet, se non espressamente autorizzato dal Conservatorio G Puccini.

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 dal titolare e con il rispetto delle normali procedure di acquisto.

È da evitare ogni forma di registrazione a siti i cui contenuti non siano legati all'attività lavorativa.

È vietata la partecipazione a Forum non professionali, l'utilizzo di chat line (esclusi gli strumenti autorizzati), di bacheche elettroniche e le registrazioni in guest books anche utilizzando pseudonimi (o nicknames).

#### **i) Telefonia mobile.**

L'uso del telefono cellulare può essere concesso dal Conservatorio G Puccini alle figure professionali che per la natura delle prestazioni e dell'incarico richiedano pronta e costante reperibilità in luoghi diversi dalla sede di lavoro o quando sussistano particolari ed indifferibili esigenze di comunicazione che non possono essere soddisfatte con gli strumenti di telefonia fissa e posta elettronica. La concessione del telefono cellulare è disposta dal legale rappresentante. In nessun caso può essere concesso il telefono di servizio a soggetti esterni all'Amministrazione (collaboratori, consulenti, volontari, dipendenti di imprese appaltatrici). Lo Conservatorio G Puccini provvede alla fornitura dei telefoni cellulari e all'attivazione delle relative utenze e sia il terminale, sia la SIM card e la relativa utenza sono concessi in uso al dipendente e/o amministratore fino ad esplicita revoca, con conseguente ritiro del materiale fornito e disattivazione dell'utenza. I telefoni cellulari sono di uso personale e non possono essere ceduti a terzi a nessun titolo. Gli utilizzatori dei telefoni cellulari, affinché possano essere immediatamente rintracciabili nei casi di necessità, hanno l'obbligo di mantenere in funzione il telefono cellulare durante le ore di servizio, durante le ore di reperibilità, ove previste, ed in tutti i casi in cui le circostanze concrete lo rendano opportuno. La durata delle chiamate deve essere la più contenuta possibile in relazione alle esigenze di servizio, preferendo altresì la funzione dei messaggi di testo in caso di brevi comunicazioni. Qualora il possessore di telefono cellulare si trovi negli uffici del Conservatorio, è fatto obbligo di utilizzare gli apparecchi della rete fissa per comunicare con altri apparecchi di rete fissa. Ogni assegnatario di telefono cellulare di servizio è tenuto all'uso appropriato e alla diligente conservazione dell'apparecchio e alla piena conoscenza delle disposizioni di utilizzo previste. In caso di furto o smarrimento dell'apparecchio, l'assegnatario dovrà darne immediata comunicazione al Conservatorio G Puccini ai fini dell'immediato blocco dell'utenza. Se il furto o lo smarrimento si verificano in circostanze in cui non è possibile comunicare con il Conservatorio, l'assegnatario dovrà provvedere personalmente al blocco della SIM contattando il gestore di telefonia mobile. L'assegnatario dovrà successivamente presentare la formale denuncia di furto o smarrimento e farne pervenire copia al Conservatorio. In caso di malfunzionamento o di guasto dell'apparecchio o della SIM l'assegnatario dovrà rivolgersi al Conservatorio G Puccini. Verranno predisposti dei monitoraggi periodici sul rendiconto telefonico, al fine di ottemperare al contenimento e al monitoraggio della spesa: il ..... è incaricato della visione delle fatture telefoniche e alla segnalazione di anomalie di traffico. In caso non si rilevino delle anomalie si procederà con l'apposizione sulle bollette telefoniche del visto favorevole e si disporrà il pagamento. Quando dall'esame del traffico di una singola utenza si rileva uno scostamento significativo rispetto alla media del consumo, il ..... lo segnala all'utilizzatore medesimo con richiesta di verifica e di attestazione che le telefonate risultanti dal tabulato analitico sono state effettuate per motivi di servizio. In caso di esito positivo il ..... autorizzerà il pagamento delle spese, in caso di esito negativo il traffico in eccesso sarà a carico del consegnatario.

#### **ISTRUZIONI PER L'USO DEGLI STRUMENTI "NON ELETTRONICI"**

Per "non elettronici" si intendono sia documenti cartacei sia documenti di altro tipo come ad esempio microfilm, microfiches e lucidi. I documenti di questo tipo contenenti dati particolari (ex dati sensibili) o giudiziari devono essere protetti in appositi armadi dotati di chiavi. Tutti i documenti contenenti dati particolari (ex dati sensibili) o giudiziari che si ritiene debbano essere eliminati devono essere distrutti e non gettati nei cestini.

Per proteggere i dati personali è opportuno evitare il deposito di documenti di qualsiasi genere negli ambienti di transito o pubblici (corridoi o sale riunioni), come pure l'abbandono in vista sulle scrivanie quando ci si debba assentare dal proprio posto di lavoro.

#### **Distruzione delle copie cartacee**

Coloro che sono preposti alla duplicazione di documentazione (con stampanti o fotocopiatrici o altre periferiche) ovvero che utilizzando strumenti per la riproduzione cartacea di documenti digitali, sono tenuti a procedere alla relativa distruzione del supporto, qualora si verificano errori o la riproduzione non sia corretta, evitando di riutilizzare i fogli, salva l'ipotesi di uso esclusivamente personale per eventuali appunti o brutte copie, da distruggere immediatamente quando non più necessarie;

#### **Misure di sicurezza**

Il trattamento sicuro di documenti contenenti Dati Personali richiede la presenza di misure di sicurezza con le quali l'Incaricato possa interagire ed una serie di accorgimenti direttamente gestibili dall'Incaricato stesso. In particolare, si richiede:

- la presenza e l'uso tassativo di armadi e cassetti dotati di serratura adeguata;
- la presenza e l'uso tassativo, ove si richieda la distruzione di documenti contenenti dati particolari (ex dati sensibili) e giudiziari, di un trita-documenti.

#### **Prescrizioni per gli incaricati**

L'Incaricato deve attenersi alle seguenti prescrizioni:

- in nessun caso è concesso l'accesso a documentazione contenente Dati Personali per motivi non dettati da esigenze di lavoro strettamente connesse ai trattamenti dichiarati, autorizzati e tutelati dal Titolare;
- la documentazione contenente Dati Personali che, per ragioni di praticità operativa, risiede sulle scrivanie degli Incaricati, deve comunque essere rimossa al termine dell'orario di lavoro;
- l'accesso ai supporti deve essere limitato al tempo necessario a svolgere i Trattamenti previsti;
- i supporti devono essere archiviati in ambiente ad accesso controllato;
- i documenti contenenti dati personali, non devono essere lasciati incustoditi in un ambiente non controllato (ad es. a seguito della stampa dei documenti su stampante di rete);
- il numero di copie di documenti contenenti Dati Personali deve essere strettamente funzionale alle esigenze di lavoro;
- cassetti ed armadi contenenti documentazione riservata debbono tassativamente essere chiusi a chiave fuori dell'orario di lavoro;
- l'accesso fuori orario lavorativo a documenti contenenti Dati particolari (ex dati sensibili) /giudiziari può avvenire da parte di personale Incaricato, o tramite autorizzazione di quest'ultimo, unicamente previa registrazione dell'accesso a tali documenti;
- la distruzione di documenti contenenti Dati Personali deve essere operata, ove possibile, direttamente dal personale Incaricato;
- ove non siano disponibili strumenti per la distruzione dei documenti (trita documenti), o il volume di questi sia tale da imporre il ricorso al servizio di macero, il personale Incaricato che avvia al macero la documentazione è tenuto a confezionare tale documentazione in modo che il pacco risulti anonimo e solido;
- quando gli atti e i documenti contenenti dati personali, dati particolari (ex dati sensibili) o giudiziari sono affidati agli Incaricati per lo svolgimento dei relativi compiti, i medesimi atti e documenti sono controllati e custoditi dagli Incaricati fino alla restituzione in maniera

che ad essi non accedano persone prive di autorizzazione, e sono restituiti al termine delle operazioni affidate;

• l'accesso agli archivi contenenti dati particolari (ex dati sensibili) o giudiziari deve essere controllato. Le persone ammesse, a qualunque titolo, dopo l'orario di chiusura, sono identificate e registrate. Quando gli archivi non sono dotati di strumenti elettronici per il controllo degli accessi o di incaricati della vigilanza, le persone che vi accedono devono essere preventivamente autorizzate.

• è severamente vietato utilizzare documenti contenenti Dati personali, dati particolari (ex dati sensibili) o giudiziari come carta da riciclo o da appunti.

#### **ADDETTI ALLA MANUTENZIONE**

Le seguenti istruzioni devono essere osservate dai preposti in qualità di addetti alla gestione o manutenzione che trattano dati di titolarità per i quali è nominato un responsabile del trattamento nonché dagli addetti di ditte specializzate che svolgano interventi tecnici di gestione e manutenzione degli strumenti elettronici:

- Effettuare operazioni di manutenzione e supporto per verifica corretto funzionamento (monitoraggio e diagnostica) su flussi dei dati;
- gestire le credenziali di autenticazione dei soggetti incaricati del trattamento su indicazione dell'Amministratore di sistema;
- gestire i profili di autorizzazione degli incaricati al trattamento dei dati, su specifiche impartite dai responsabili di funzione/BU, su indicazione dell'Amministratore di sistema;
- provvedere alla disattivazione/variazione delle utenze, ivi compreso l'account di posta elettronica, assegnate al personale cessato dal servizio o che abbia modificato il proprio ambito di trattamento, su richiesta specifica dei responsabili ovvero della Direzione Risorse Umane e su indicazione dell'Amministratore di sistema;
- custodire la documentazione cartacea, prodotta nello svolgimento dei propri compiti istituzionali;

L'accesso agli addetti alla gestione e manutenzione è consentito unicamente ai soli dati personali la cui conoscenza sia strettamente necessaria per adempiere alle operazioni di manutenzione dei programmi o del sistema informatico.

A ciascun addetto alla manutenzione, previa sottoscrizione di apposito atto per accettazione, è pertanto consentito eseguire le operazioni strettamente necessarie a tali scopi e/o richieste dal titolare, secondo le seguenti istruzioni operative:

- Nel caso in cui sia necessario effettuare stampe di prova per controllare il funzionamento di stampanti o per verificare il funzionamento di strumenti o programmi installati, non utilizzare files già esistenti ma creare files di prova.
- Nel caso si renda strettamente necessario accedere a files contenenti dati (ad esempio per il recupero di un testo) limitare l'accesso ai dati per il tempo strettamente necessario all'assolvimento delle operazioni di manutenzione.
- Per effettuare operazioni di manutenzione sui database del Conservatorio G Puccini che prevedano la raccolta e la conservazione dei dati, tali dati dovranno essere custoditi in modo tale da non essere accessibili da soggetti non autorizzati.
- Devono inoltre essere adottate le misure di sicurezza minime previste dal codice in materia di protezione dei dati personali;
- E' necessario informare al più presto il titolare o il responsabile del trattamento qualora si dovessero riscontrare malfunzionamenti o non conformità.

• Tutti i dati personali contenuti nei data base devono essere protetti da password;

• Nel caso in cui sia necessario accedere ai dati attraverso gli strumenti elettronici in dotazione agli incaricati, attenersi alle seguenti indicazioni:

o in presenza dell'incaricato, far digitare la password dall'incaricato stesso evitando di venire a conoscenza;

o in assenza dell'incaricato rivolgersi alla persona individuata dall'incaricato quale proprio fiduciario il quale provvederà all'inserimento della password.

• Nei casi in cui sia necessario accedere ai dati personali attraverso il server, rivolgersi all'amministratore di sistema o provvedere, in collaborazione con l'amministratore di sistema stesso, alla creazione di credenziali di autenticazione da utilizzarsi esclusivamente per l'accesso da parte degli addetti alla manutenzione/gestione dei sistemi informatici;

• L'amministratore di sistema ha facoltà, in qualunque momento di controllare e verificare l'operato degli addetti alla manutenzione;

• Qualora si renda necessario prelevare apparecchiature elettroniche per effettuare attività di ripristino o interventi di manutenzione che comportino il reset di password precedentemente individuate, la nuova password di accesso sarà comunicata all'incaricato il quale provvederà a cambiarla al termine delle operazioni di manutenzione;

• l'accesso al sistema informatico da parte degli addetti alla manutenzione/gestione del sistema è consentito unicamente previo inserimento di password e ID;

• E' assolutamente vietato comunicare o diffondere i dati personali di qualsiasi natura provenienti dai database gestiti dalla società, se non previa espressa comunicazione scritta;

• Nel caso in cui ci si avvalga di soggetti esterni per interventi specialistici che comportino trattamento di dati personali deve essere rilasciata una dichiarazione scritta dell'intervento effettuato che ne attesta la conformità alle disposizioni in materia di misure minime di sicurezza

#### **OSSERVANZA DELLE DISPOSIZIONI IN MATERIA DI PROTEZIONE DATI PERSONALI**

È obbligatorio attenersi alle disposizioni in materia di protezione dati personali e di misure minime di sicurezza, ai sensi del GDPR 2016/679.

#### **NON OSSERVANZA DELLA NORMATIVA DEL CONSERVATORIO G PUCCINI**

Il mancato rispetto o la violazione delle regole contenute nel presente regolamento è perseguibile con provvedimenti disciplinari nonché con le azioni civili e penali consentite.

#### **AGGIORNAMENTO E REVISIONE**

Tutti gli utenti possono proporre, quando ritenuto necessario, integrazioni al presente Regolamento. Le proposte verranno esaminate dal Titolare.

Il presente Regolamento è soggetto a revisione con frequenza annuale.

Data \_\_\_\_\_

**Il Titolare del trattamento**

**Presidente *pro tempore*  
Avv. Maurizio Sergi**

**Data e firma per ricevuta comunicazione .....**