
	Documento gestione privacy Disposizione sull'uso di device, internet, posta elettronica ed archivi cartacei	01_02Disciplinare_uso_strumenti_informatici		
		Rev.	Data	Foglio
		02	23/07/2025	1 di 16

Regole di condotta ed obblighi dei dipendenti e dei collaboratori in relazione all'uso degli strumenti informatici, di Internet e della Posta Elettronica, redatto ai sensi del Reg. EU 2016/679 (Regolamento Generale sulla Protezione dei Dati) ed in osservanza alla deliberazione del Garante per la protezione dei dati personali n. 13 del 1/3/07.

Rev.	Data	Motivo Revisione	Emissione: Titolare del Trattamento
0	30/05/18	Prima Emissione	Fondazione Teatro Massimo
1	19/04/2024	Inserimento del paragrafo 27	
2	23/07/2025	Aggiornamento misure di sicurezza ICT	

Indice del documento:

1.	<i>Riferimenti e definizioni</i>	2
2.	<i>Premessa.....</i>	2
3.	<i>Autorizzazione all'uso degli strumenti informatici</i>	3
4.	<i>Titolarietà dei dispositivi e dei dati.....</i>	4
5.	<i>Finalità nell'utilizzo dei dispositivi.....</i>	4
6.	<i>Restituzione dei dispositivi.....</i>	4
7.	<i>Restituzione dei dati cartacei.....</i>	4
8.	<i>Le Password</i>	4
9.	<i>Regole per la corretta gestione delle password.....</i>	5
10.	<i>Login e Logout.....</i>	6
11.	<i>Obblighi relativi all'uso dei dispositivi.....</i>	6
12.	<i>Modalità d'uso del PC aziendale.....</i>	7
13.	<i>Antivirus e sistemi di sicurezza centralizzati e gestiti</i>	8
15.	<i>La Posta Elettronica è uno strumento di lavoro.....</i>	10
16.	<i>L'utilizzo del notebook, tablet o smartphone.....</i>	12
17.	<i>Memorie esterne (chiavi usb, hard disk, memory card, cd-rom, dvd, ecc.)</i>	12
18.	<i>Utilizzo del cellulare/smartphone personale.</i>	13
19.	<i>Utilizzo di sistemi cloud.....</i>	13
20.	<i>Organizzazione della scrivania.....</i>	13
21.	<i>In caso di furto</i>	14
22.	<i>Controlli.....</i>	14
23.	<i>Modalità di verifica</i>	14
24.	<i>Modalità di Conservazione.....</i>	15
25.	<i>Segreto aziendale.....</i>	15
26.	<i>Individuazione dei Soggetti autorizzati.....</i>	15
27.	<i>Conseguenze delle infrazioni disciplinari</i>	15

	Documento gestione privacy Disposizione sull'uso di device, internet, posta elettronica ed archivi cartacei	01_02Disciplinare_uso_strumenti_informatici		
		Rev.	Data	Foglio
		02	23/07/2025	2 di 16

28.	Modalità di Esercizio dei diritti	16
29.	Validità, aggiornamento e diffusione	16

1. Riferimenti e definizioni

Reg. UE 2016/679 - GDPR: REGOLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati).

Provvedimenti del Garante della protezione dei dati personali:

- Deliberazione 23 novembre 2006 (G.U. 7 dicembre 2006, n. 285) “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”.
- Deliberazione n. 13 del 1/3/2007 – (GU n° 58 del 10 marzo 2007) “Linee guida del Garante per posta elettronica e internet”.
- Provvedimento del 27 novembre 2008 “Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema”.
- Provvedimento n. 547 del 22 dicembre 2016 “Accesso alla posta elettronica dei dipendenti”.
- Circolare AGID n. 2/2017 del 18 aprile 2017 “Misure minime di sicurezza ICT per le pubbliche amministrazioni”.

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.

Dispositivi aziendali: computer, portatili, smart phone, palmari, o qualsiasi altro strumento informatico di proprietà della Fondazione Teatro Massimo o comunque in uso per lo svolgimento delle attività lavorative.

Dipendente: personale assunto con qualsiasi tipo di forma contrattuale, anche in stage o tirocinio.


Autorizzato: ogni dipendente, come sopra identificato, ed ogni consulente esterno che, nell'ambito dell'attività assegnatagli, tratta dati (nell'accezione del capitolo seguente) riferiti alla Fondazione Teatro Massimo.

2. Premessa

Durante l'attività lavorativa, i dipendenti e collaboratori della Fondazione Teatro Massimo, si ritrovano a gestire una serie di “**informazioni**”, proprie e di terzi, per poter espletare la loro mansione.

Tali informazioni possono essere considerate, ai sensi del Reg. UE 2016/679 “**dati personali**” quando sono riferite a persone fisiche e, per la loro gestione (Trattamento), sia cartacea che digitale, è necessario che la Fondazione Teatro Massimo adotti una serie di misure minime ed idonee previste dalle norme.

Altre informazioni, pur non essendo “dati personali” ai sensi di legge, sono in tutto e per tutto “**informazioni riservate**”, ovvero informazioni tecniche, commerciali, contrattuali, di business o di altro

	Documento gestione privacy Disposizione sull'uso di device, internet, posta elettronica ed archivi cartacei	01_02Disciplinare_uso_strumenti_informatici		
		Rev.	Data	Foglio
		02	23/07/2025	3 di 16

genere per le quali la Fondazione è chiamata a garantire la riservatezza, per una più ampia tutela del patrimonio della Fondazione.

Ai fini di questo disciplinare si specifica, pertanto, che con il termine “**dati**” deve intendersi l’insieme più ampio di informazioni di cui un dipendente o un collaboratore può venire a conoscenza e di cui deve garantire la riservatezza e la segretezza e non solo i “dati personali” intesi a norma di legge.

Inoltre, nell’ambito della sua attività, la Fondazione Teatro Massimo tratta “**dati cartacei**” ovvero informazioni su supporto cartaceo e “**dati digitali**” ovvero informazioni che vengono memorizzate o semplicemente transitano attraverso apparecchiature digitali.

In linea generale, ogni dato, nell’accezione più ampia sopra descritta, di cui l’incaricato viene a conoscenza, nell’ambito della propria attività lavorativa, è da considerarsi riservato e non deve essere comunicato o diffuso a nessuno (anche una volta interrotto il rapporto lavorativo con la Fondazione o qualora parte delle informazioni siano di pubblico dominio) salvo specifica autorizzazione esplicita della Fondazione Teatro Massimo.

Anche tra colleghi, oppure tra dipendenti e collaboratori esterni, è necessario adottare la più ampia riservatezza nella comunicazione dei dati conosciuti, limitandosi solo a quei casi che si rendono necessari per espletare al meglio l’attività lavorativa richiesta.

La progressiva diffusione delle nuove tecnologie informatiche ed in particolare l’accesso alla rete internet dal computer aziendale, espone la Fondazione Teatro Massimo a possibili rischi di un coinvolgimento di rilevanza sia civile, sia penale, sia amministrativa, creando problemi alla sicurezza e all’immagine della Fondazione.

Premesso che i comportamenti che normalmente si adottano nell’ambito di un rapporto di lavoro, tra i quali rientrano l’utilizzo delle risorse informatiche e telematiche, devono sempre ispirarsi al principio di diligenza e correttezza, la Fondazione Teatro Massimo ha adottato il presente Disciplinare Interno diretto ad evitare che condotte inconsapevoli possano innescare problemi o minacce alla sicurezza dei dati o delle attrezzature aziendali.

Il presente Disciplinare Interno si applica agli **Incaricati (persone autorizzate al trattamento dei dati personali sotto l’autorità diretta del titolare ex art. 4 GDPR)** che si trovino a trattare dati di qualsiasi natura, sia che abbiano ricevuto in consegna un dispositivo aziendale, sia che effettuino trattamenti esclusivamente cartacei o con strumenti informatici non ad uso esclusivo.

Una gestione dei dati cartacei, un uso dei COMPUTER e di altri dispositivi elettronici (di seguito Dispositivo) nonché dei servizi di internet e della posta elettronica difforme dalle regole contenute nel presente Disciplinare potrebbe esporre la Fondazione ad aumentare la minaccia di accessi non autorizzati ai dati e/o al sistema informatico aziendale, furti o divulgazioni di informazioni riservate, nonché furti o danneggiamenti del sistema informatico e/o malfunzionamenti in generale dell’intero sistema informatico.

Le informazioni contenute nel presente Disciplinare vengono rilasciate anche ai sensi dell’art. 13 del Reg. UE 2016/679 e costituiscono, quindi, parte integrante dell’informativa rilasciata agli Incaricati.


3. Autorizzazione all’uso degli strumenti informatici

All’inizio del rapporto lavorativo o di consulenza, la Fondazione Teatro Massimo valuta la presenza dei presupposti per l’autorizzazione all’uso dei vari dispositivi aziendali, di internet e della posta elettronica da parte degli incaricati.

Successivamente e periodicamente la Fondazione valuta la permanenza dei presupposti per l’utilizzo dei dispositivi aziendali, di internet e della posta elettronica.

È fatto esplicito divieto, ai soggetti non autorizzati, di accedere agli strumenti informatici aziendali.

Hanno diritto all’utilizzo degli strumenti e ai relativi accessi solo gli incaricati che, per funzioni lavorative, ne abbiano un effettivo e concreto bisogno.

	Documento gestione privacy Disposizione sull'uso di device, internet, posta elettronica ed archivi cartacei	01_02Disciplinare_uso_strumenti_informatici		
		Rev.	Data	Foglio
		02	23/07/2025	4 di 16

Si sottolinea che le limitazioni alle autorizzazioni sono attuate in Fondazione, anche alla luce del Provvedimento del Garante 1/03/07 che indica di ridurre a titolo cautelativo e preventivo l'utilizzo degli strumenti informatici in considerazione dei pericoli e delle minacce indicate in questo documento.

4. Titolarità dei dispositivi e dei dati

La Fondazione Teatro Massimo è esclusiva titolare e proprietaria dei Dispositivi messi a disposizione degli Incaricati ai soli fini dell'attività lavorativa; è, inoltre, l'unica esclusiva titolare e proprietaria di tutte le informazioni, le registrazioni ed i dati contenuti e/o trattati mediante i propri dispositivi digitali o archiviati in modo cartaceo nei propri locali.

L'incaricato non può ritenere che le informazioni, le registrazioni ed i dati da lui trattati o memorizzati nei dispositivi aziendali (inclusi i messaggi di posta elettronica e/o chat inviati o ricevuti, i file di immagini, i files di filmati o altre tipologie di files) siano privati o personali, né può presumere che dati cartacei in suo possesso possano essere da lui copiati, comunicati o diffusi senza l'autorizzazione della Fondazione.

5. Finalità nell'utilizzo dei dispositivi

I dispositivi assegnati sono uno strumento lavorativo nelle disponibilità dell'Incaricato esclusivamente per un fine di carattere lavorativo. I dispositivi, quindi, non devono essere utilizzati per finalità private e diverse da quelle aziendali, se non eccezionalmente e nei limiti evidenziati dal presente Disciplinare. Qualsiasi eventuale tolleranza da parte di questa Fondazione, apparente o effettiva, non potrà, comunque, legittimare comportamenti contrari alle istruzioni contenute nel presente Disciplinare.

6. Restituzione dei dispositivi

A seguito di una cessazione del rapporto lavorativo o di consulenza dell'Incaricato con la Fondazione o, comunque, al venir meno, ad insindacabile giudizio della Fondazione Teatro Massimo, della permanenza dei presupposti per l'utilizzo dei dispositivi aziendali, gli incaricati hanno i seguenti obblighi:

1. Procedere immediatamente alla restituzione dei dispositivi in uso;
2. Divieto assoluto di formattare o alterare o manomettere o distruggere i dispositivi assegnati o rendere inintelligibili i dati in essi contenuti tramite qualsiasi processo.

7. Restituzione dei dati cartacei

A seguito di una cessazione del rapporto lavorativo o di consulenza dell'Incaricato con la Fondazione o, comunque, al venir meno, ad insindacabile giudizio della Fondazione Teatro Massimo, della permanenza dei presupposti per l'utilizzo di dati cartacei aziendali, gli incaricati hanno i seguenti obblighi:


1. Procedere immediatamente alla restituzione dei dati cartacei in loro possesso;
2. Divieto assoluto di alterare o manomettere o distruggere i dati cartacei assegnati o renderli inintelligibili tramite qualsiasi processo.

8. Le Password

Le password sono un metodo di autenticazione assegnato dalla Fondazione per garantire l'accesso protetto ad uno strumento hardware oppure ad un applicativo software.

La prima caratteristica di una password è la segretezza, e cioè il fatto che non venga svelata ad altri soggetti. La divulgazione delle proprie password o la trascuratezza nella loro conservazione può causare gravi danni al proprio lavoro, a quello dei colleghi ed alla Fondazione Teatro Massimo nel suo complesso.

La Fondazione Teatro Massimo ha implementato alcuni meccanismi che permettono di aiutare e supportare gli Incaricati in una corretta gestione delle password, in particolare, per quanto riguarda le password di accesso al Dominio, è in funzione un sistema automatico di richiesta di aggiornamento delle stesse impostato, secondo il livello di sicurezza richiesto della Fondazione stessa e, comunque, in linea con quanto richiesto dalla normativa privacy.

	Documento gestione privacy Disposizione sull'uso di device, internet, posta elettronica ed archivi cartacei	01_02Disciplinare_uso_strumenti_inf ormatici		
		Rev.	Data	Foglio
		02	23/07/2025	5 di 16

Altra buona norma è quella di non memorizzare la password su supporti facilmente intercettabili da altre persone. Il miglior luogo in cui conservare una password è la propria memoria.

Le password che non vengono utilizzate da parte degli incaricati per un periodo superiore ai sei mesi verranno disattivate dalla Fondazione Teatro Massimo.

In qualsiasi momento la Fondazione si riserva il diritto di revocare all'Incaricato il permesso di accedere ad un sistema hardware o software a cui era precedentemente autorizzato, rimuovendo user id o modificando/cancellando la password ad esso associata.

9. Regole per la corretta gestione delle password

A ciascun incaricato è affidato l'utilizzo e l'accesso ad un PC Client dotato di un sistema di autenticazione informatica, sistema che costituisce una delle regole tecniche a tutela dei dati di grande importanza.

In particolare, è previsto l'utilizzo da parte degli Incaricati di apposite credenziali che consentono il superamento di una procedura di autenticazione relativa a uno specifico trattamento o a un insieme di trattamenti.

Ciascun Incaricato è reso edotto del fatto che le credenziali di autenticazione sono personali:

- devono essere memorizzate;
- non devono essere comunicate a nessuno;
- non devono essere trascritte.

Le "credenziali di autenticazione" consistono in un codice per l'identificazione dell'incaricato("user id") non assegnabile, neppure successivamente nel tempo, ad altro incaricato.

La credenziale di autenticazione deve essere associata a una parola chiave riservata conosciuta solamente dal medesimo ("password"), composta da almeno 8 (otto) caratteri, non contenente riferimenti agevolmente riconducibili all'incaricato.

La password, in particolare, deve rispettare i seguenti criteri:

<ul style="list-style-type: none"> • non deve contenere nomi comuni; • non deve contenere nomi di persona; • non deve essere riconducibile all'incaricato del trattamento; • non deve essere uguale alla user-id; 	<ul style="list-style-type: none"> • deve contenere sia lettere che numeri; • deve comprendere almeno 3 caratteri alfabetici; • deve comprendere almeno 2 caratteri numerici e due caratteri speciali; • deve essere lunga 8 caratteri od al numero massimo consentito dal sistema di autenticazione.
---	---

Agli incaricati è prescritta la modifica della password almeno ogni tre mesi. Agli incaricati è prescritto di adottare le necessarie cautele per assicurare la segretezza della password.

L'autenticazione dell'incaricato avviene tramite la verifica della "password" relativa alla "user-id" associata.


E' previsto un sistema di "password lock-out" che blocca la procedura di accesso al Personal Computer in seguito al verificarsi di un determinato numero di accessi falliti.

Tutti tentativi di accesso non autorizzati sono registrati.

L'amministratore di sistema provvede, ogni sei mesi, alla pulizia degli account per la disattivazione delle credenziali inutilizzate nel periodo, o riferite ad incaricati che hanno perso le qualità per accedere ai dati personali.

In caso di smarrimento della password l'utente deve tempestivamente richiedere una nuova procedura di assegnazione all'amministratore di sistema.

Questa procedura garantisce l'impossibilità di collegarsi ai sistemi, usando l'identità dell'incaricato senza compiere azioni che non risultino evidenti all'incaricato stesso.

	Documento gestione privacy Disposizione sull'uso di device, internet, posta elettronica ed archivi cartacei	01_02Disciplinare_uso_strumenti_inf ormatici		
		Rev.	Data	Foglio
		02	23/07/2025	6 di 16

Infatti, al suo rientro in Fondazione, successivo ad un eventuale intervento, l'incaricato non può connettersi con la sua password, risultando quindi automaticamente avvisato dell'avvenuto intervento il quale, in ogni caso deve essere comunicato.

La password ideale deve essere complessa, senza alcun riferimento, ma facile da ricordare. Una possibile tecnica è usare sequenze di caratteri prive di senso evidente, ma con singoli caratteri che formano una frase facile da memorizzare (es.: "NIMzz5DICmm!", Nel Mezzo Del Cammin, più il carattere 5 e il punto esclamativo). Decifrare una parola come questa può richiedere giorni, una come "radar" meno di dieci secondi. Alcuni esempi di password assolutamente da evitare:

1. Se Username = "mariorossi", password = "mario", o ancora peggio, password = "mariorossi";
2. Il nome della moglie/marito, fidanzato/a, figli, ecc. anche a rovescio;
3. La propria data di nascita, quella del coniuge, ecc.;
4. Targa della propria auto;
5. Numero di telefono proprio, del coniuge, ecc.;
6. Parole comuni tipo "Kilimangiaro", "Password", "Qwerty", "12345678" (troppo facili);
7. Qualsiasi parola del vocabolario (di qualsiasi lingua diffusa, come inglese, italiano, ecc.).

10. Login e Logout

Il "Login" è l'operazione con la quale l'Incaricato si connette al sistema informativo aziendale o ad una parte di esso, dichiarando il proprio Username e Password (ossia l'Account), aprendo una sessione di lavoro. In molti casi è necessario effettuare più login, tanti quanti sono gli ambienti di lavoro (ad es. applicativi web, Intranet), ognuno dei quali richiede un username e una password.

In questi casi, sebbene sia preferibile che ogni utente abbia un suo specifico user name e password, la Fondazione Teatro Massimo potrà assegnare un univoco user name e password per gruppi di incaricati per l'accesso alla macchina fisica, mentre rimarranno separati ed univoci per l'accesso agli applicativi che contengono dati.

Il "Logout" è l'operazione con cui viene chiusa la sessione di lavoro. Al termine della giornata lavorativa, tutte le applicazioni devono essere chiuse secondo le regole previste dall'applicazione stessa. La non corretta chiusura può provocare una perdita di dati o l'accesso agli stessi da parte di persone non autorizzate.


Il "blocco del computer" è l'operazione con cui viene impedito l'accesso alla sessione di lavoro (tastiera e schermo disattivati) senza chiuderla, tale blocco sarà attivato automaticamente a seguito di un tempo predeterminato di mancato utilizzo.

11. Obblighi relativi all'uso dei dispositivi

L'utilizzo dei dispositivi fisici e la gestione dei dati ivi contenuti devono svolgersi nel rispetto della sicurezza e dell'integrità del patrimonio dati aziendale.

L'incaricato deve quindi eseguire le operazioni seguenti:

1. Se si allontana dalla propria postazione dovrà mettere in protezione il suo dispositivo, affinché persone non autorizzate non abbiano accesso ai dati protetti;
2. Bloccare il suo dispositivo prima delle pause e, in generale, ogni qualvolta abbia bisogno di allontanarsi dalla propria postazione;
3. Chiudere la sessione (Logout) a fine giornata;
4. Spegnere il PC dopo il Logout;
5. Controllare sempre che non vi siano persone non autorizzate alle sue spalle che possano prendere visione delle schermate del suo dispositivo.

	Documento gestione privacy Disposizione sull'uso di device, internet, posta elettronica ed archivi cartacei	01_02Disciplinare_uso_strumenti_inf ormatici		
		Rev.	Data	Foglio
		02	23/07/2025	7 di 16

12. Modalità d'uso del PC aziendale

Il sistema informativo aziendale è composto da un insieme di unità server centrali e macchine client connessi ad una rete locale (LAN), che utilizzano diversi sistemi operativi e applicativi.

E' consigliabile salvare a fine giornata sul sistema di repository documentale centralizzato i files creati, elaborati o modificati sul computer assegnato. La Fondazione Teatro Massimo non effettua il backup dei dati memorizzati in locale.

Il computer consegnato all'incaricato è uno strumento di lavoro e contiene tutti i software necessari a svolgere le attività affidate. Ogni utilizzo non inerente all'attività lavorativa può contribuire ad innescare disservizi, rallentamenti del sistema, 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. Il computer che viene consegnato contiene tutti i software necessari a svolgere le attività affidate dalla Fondazione. Per necessità aziendali, gli amministratori di sistema, utilizzando il proprio login con privilegi di amministratore e la password dell'amministratore, potranno accedere, con le regole indicate nel presente documento, sia alle memorie di massa locali di rete (repository e backup) che ai server aziendali nonché, previa comunicazione al dipendente, accedere al computer, anche in remoto.


In particolare l'Incaricato deve adottare le seguenti misure:

1. Utilizzare solo ed esclusivamente le aree di memoria della rete della Fondazione Teatro Massimo ed ivi creare e registrare file e software o archivi dati, senza pertanto creare altri files fuori dalle unità di rete;
2. Spegnerne il computer, o curarsi di effettuare il Logout, ogni sera prima di lasciare gli uffici o in caso di assenze prolungate, poiché lasciare un elaboratore 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;
3. Mantenere sul computer esclusivamente i dispositivi di memorizzazione, comunicazione o altro (come ad esempio masterizzatori), disposti dalla Fondazione;
4. Non dare accesso al proprio computer ad altri utenti, a meno che siano incaricati con cui condividono l'utilizzo dello stesso Pc o a meno di necessità stringenti e sotto il proprio costante controllo.

Divieti Espresi sull'utilizzo del PC

All'incaricato è vietato:

1. La gestione, la memorizzazione (anche temporanea) o il trattamento di file, documenti e/o informazioni personali dell'incaricato o comunque non afferenti alle attività lavorative nella rete, nel disco fisso o in altre memorie di massa aziendali e negli strumenti informatici aziendali in genere.
2. Modificare le configurazioni già impostate sul personal computer.
3. Utilizzare programmi e/o sistemi di criptazione senza la preventiva autorizzazione scritta della Fondazione Teatro Massimo.
4. Installare alcun software di cui la Fondazione Teatro Massimo non possieda la licenza, né installare alcuna versione diversa, anche più recente, rispetto alle applicazioni o al sistema operativo presenti sul personal computer consegnato, senza l'espressa autorizzazione dell'organizzazione. Né è, peraltro, consentito fare copia del software installato al fine di farne un uso personale.
5. Caricare sul disco fisso del computer o nel server alcun documento, gioco, file musicale o audiovisivo o immagine diversi da quelli necessari allo svolgimento delle mansioni affidate.
6. Aggiungere o collegare dispositivi hardware (ad esempio hard disk, driver, PCMCIA, ecc.) o periferiche (telecamere, macchine fotografiche, smartphone, chiavi USB ecc.) diversi da quelli consegnati, senza l'autorizzazione espressa da parte della Fondazione.
7. Creare o diffondere, intenzionalmente o per negligenza, programmi idonei a danneggiare il sistema informatico della Fondazione, quali per esempio virus, trojan horse ecc.
8. Accedere, rivelare o utilizzare informazioni non autorizzate o comunque non necessarie per le mansioni svolte.
9. Effettuare in proprio attività manutentive.

	Documento gestione privacy Disposizione sull'uso di device, internet, posta elettronica ed archivi cartacei	01_02Disciplinare_uso_strumenti_inf ormatici		
		Rev.	Data	Foglio
		02	23/07/2025	8 di 16


10. Permettere attività manutentive da parte dei soggetti non espressamente autorizzati da parte della Fondazione.

13. Antivirus e sistemi di sicurezza centralizzati e gestiti

Per garantire la sicurezza dei dispositivi aziendali, dei dati e dell'ambiente digitale in cui operiamo, è stato implementato un sistema centralizzato di antivirus, RMM (Remote Monitoring and Management) e Network Scan di rete. Questi strumenti permettono il monitoraggio tecnico e la protezione dei sistemi informatici da minacce informatiche, vulnerabilità e malfunzionamenti, contribuendo alla continuità operativa e alla tutela delle informazioni aziendali. L'uso di tali strumenti è conforme alla normativa vigente in materia di privacy e tutela del lavoratore: non viene effettuato alcun controllo sull'attività personale o sui contenuti non pertinenti al lavoro, e i dati acquisiti e trattati sono esclusivamente quelli necessari a fini di sicurezza informatica, manutenzione tecnica e gestione dei dispositivi aziendali.

Per minimizzare il rischio da virus informatici, gli utilizzatori dei PC adottano le seguenti regole:

- divieto di lavorare con diritti di amministratore o superutente sui sistemi operativi che supportano la multiutenza;
- limitare lo scambio fra computer di supporti rimovibili (cd, dvd, zip) contenenti file con estensione .EXE, .COM, .OVR, .OVL, .SYS, .DOC, .XLS;
- controllare (scansionare con un antivirus aggiornato) qualsiasi supporto di provenienza sospetta prima di operare su uno qualsiasi dei file in esso contenuti;
- evitare l'uso di programmi shareware e di pubblico dominio se non se ne conosce la provenienza, ovvero divieto di "scaricare" dalla rete internet ogni sorta di file, eseguibile e non.
- disattivare la creazione di nuove finestre da parte del browser ed il loro ridimensionamento e impostare il livello di protezione su "chiedi conferma" (il browser avvisa quando uno script cerca di eseguire qualche azione);
- attivare la protezione massima per gli utenti del programma di posta Outlook al fine di proteggersi dal codice HTML di certi messaggi e-mail (buona norma e visualizzare e trasmettere messaggi in formato testo poiché alcune pagine web, per il solo fatto di essere visualizzate possono infettare il computer);
- non aprire gli allegati di posta se non si è certi della loro provenienza, e in ogni caso analizzarli con un software antivirus. Usare prudenza anche se un messaggio proviene da un indirizzo conosciuto (alcuni virus prendono gli indirizzi dalle mailing list e della rubrica di un computer infettato per inviare nuovi messaggi "infetti");
- non cliccare mai un link presente in un messaggio di posta elettronica da provenienza sconosciuta, (in quanto potrebbe essere falso e portare a un sito-truffa);
- non utilizzare le chat;
- consultare con periodicità settimanale la sezione sicurezza del fornitore del sistema operativo e applicare le patch di sicurezza consigliate;
- seguire scrupolosamente le istruzioni fornite dal sistema antivirus nel caso in cui tale sistema antivirus abbia scoperto tempestivamente il virus (in alcuni casi esso è in grado di risolvere il problema, in altri chiederà di eliminare o cancellare il file infetto);
- avvisare il Responsabile dei Sistemi Informativi nel caso in cui il virus sia stato scoperto solo dopo aver subito svariati malfunzionamenti della rete o di qualche PC, ovvero in ritardo (in questo caso è possibile che l'infezione abbia raggiunto parti vitali del sistema);
- conservare i dischi di ripristino del proprio PC (creati con l'installazione del sistema operativo, o forniti direttamente dal costruttore del PC);
- conservare le copie originali di tutti i programmi applicativi utilizzati e la copia di backup consentita per legge;
- conservare la copia originale del sistema operativo e la copia di backup consentita per legge;

	Documento gestione privacy Disposizione sull'uso di device, internet, posta elettronica ed archivi cartacei	01_02Disciplinare_uso_strumenti_informatici		
		Rev.	Data	Foglio
		02	23/07/2025	9 di 16

- conservare i driver delle periferiche (stampanti, schede di rete, monitor ecc. fornite dal costruttore).

Nel caso di sistemi danneggiati seriamente da virus l'Amministratore di Sistema procede a reinstallare il sistema operativo, i programmi applicativi ed i dati;

14. Internet è uno strumento di lavoro


La connessione alla rete internet dal dispositivo avuto in dotazione è ammessa esclusivamente per motivi attinenti allo svolgimento dell'attività lavorativa.

In particolare si vieta l'utilizzo dei social network, se non espressamente autorizzati, quale strumento di lavoro per es. di promozione dell'immagine aziendale.

La Fondazione potrà adottare idonee misure tecniche preventive volte a ridurre navigazioni a siti non correlati all'attività lavorativa attraverso filtri e black list.

Divieti Espresi concernenti Internet:

1. È vietata la navigazione nei siti che possono rivelare le opinioni politiche religiose, sindacali e di salute dell'Incaricato poiché potenzialmente idonea a rivelare dati sensibili ai sensi del Reg. UE 2016/679.
2. È fatto divieto di accedere a siti internet che abbiano un contenuto contrario a norme di legge e a norme a tutela dell'ordine pubblico, rilevante ai fini della realizzazione di una fattispecie di reato o che siano in qualche modo discriminatori sulla base della razza, dell'origine etnica, del colore della pelle, della fede religiosa, dell'età, del sesso, della cittadinanza, dello stato civile, degli handicap.
3. È vietato all'Incaricato lo scarico di software (anche gratuito) prelevato da siti Internet.
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 dal Titolare e con il rispetto delle normali procedure di acquisto.
5. È vietata 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, di bacheche elettroniche o partecipare a gruppi di discussione o lasciare commenti ad articoli o iscriversi a mailing list spendendo il marchio o la denominazione dell'organizzazione, salvo specifica autorizzazione dell'organizzazione stessa.
7. È vietata la memorizzazione di documenti informatici di natura oltraggiosa, diffamatoria e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica.
8. È vietato all'Incaricato di promuovere utile o guadagno personale attraverso l'uso di Internet o della posta elettronica aziendale.
9. È vietato accedere dall'esterno alla rete interna dell'organizzazione, salvo con le specifiche procedure previste dalla Fondazione Teatro Massimo stesso.
10. È vietato, infine, creare siti web personali sui sistemi dell'organizzazione nonché acquistare beni o servizi su Internet, a meno che l'articolo acquistato non sia stato approvato a titolo di spesa professionale.
11. È vietato accedere ad alcuni siti internet mediante azioni inibenti dei filtri, sabotando o comunque superando o tentando di superare o disabilitando i sistemi adottati dalla Fondazione Teatro Massimo per bloccare accessi non conformi all'attività lavorativa. In ogni caso è vietato utilizzare siti o altri strumenti che realizzino tale fine.
12. È vietato utilizzare l'accesso ad internet in violazione delle norme in vigore nell'ordinamento giuridico italiano a tutela del diritto d'autore (es. legge 22 aprile 1941, n. 633 e successive modificazioni, d.lgs. 6 maggio 1999, n. 169 e legge 18 agosto 2000, n. 248). In particolare, è vietato il download di materiale soggetto a copyright (testi, immagini, musica, filmati, file in genere, ...) se non espressamente autorizzato dall'organizzazione.

	Documento gestione privacy Disposizione sull'uso di device, internet, posta elettronica ed archivi cartacei	01_02Disciplinare_uso_strumenti_inf ormatici		
		Rev.	Data	Foglio
		02	23/07/2025	10 di 16

Ogni eventuale navigazione di questo tipo, comportando un illegittimo utilizzo di Internet, nonché un possibile illecito trattamento di dati personali, è posta sotto la personale responsabilità dell'Incaricato inadempiente.

15. La Posta Elettronica è uno strumento di lavoro

L'utilizzo della posta elettronica aziendale è connesso allo svolgimento dell'attività lavorativa. L'uso per motivi personali non è ammesso.

Pertanto, così come non può configurarsi un diritto del lavoratore ad accedere in via esclusiva al computer aziendale, parimenti non appare, astrattamente, prospettabile un suo diritto all'utilizzo esclusivo e riservato di una casella di posta elettronica aziendale. Talvolta, infatti, potrà essere necessario l'accesso e la lettura da parte di soggetti diversi, sempre appartenenti alla Fondazione, rispetto al suo consuetudinario utilizzatore, al fine, per esempio, di effettuare la manutenzione delle caselle di posta o di consentire la regolare continuità dell'attività della Fondazione Teatro Massimo, nelle ipotesi di sostituzioni di colleghi per ferie, malattia, etc..

Le caselle e-mail sono assegnate con natura impersonale (tipo info, amministrazione, fornitori, direttore, direttore sanitario, consulenza, ...) proprio per evitare ulteriormente che il destinatario delle mail possa considerare l'indirizzo assegnato al dipendente "privato", ai sensi dei suggerimenti del Garante a tal proposito.

Gli Incaricati assegnatari delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse.

L'organizzazione esclude la possibilità di un utilizzo personale della posta elettronica da parte degli Incaricati e allo scopo prevede che in caso di ricezione sulla e-mail aziendale di posta personale si avverte di cancellare immediatamente ogni messaggio al fine di evitare ogni eventuale e possibile back up dei dati.

Divieti Espresi

1. È vietato utilizzare l'indirizzo di posta elettronica contenente il dominio dell'organizzazione per iscriversi in qualsivoglia sito per motivi non attinenti all'attività lavorativa, senza espressa autorizzazione scritta dell'organizzazione, nonché utilizzare il dominio dell'organizzazione per scopi personali.


2. È vietato redigere messaggi di posta elettronica utilizzando l'indirizzo aziendale, diretti a destinatari esterni dell'organizzazione, senza utilizzare il seguente disclaimer:

"La Fondazione Teatro Massimo, in qualità di titolare del trattamento, desidera informarLa conformemente a quanto disposto al Reg. UE 2016/679 "Regolamento generale sulla protezione dei dati" GDPR, che il presente messaggio e gli eventuali suoi allegati sono di natura aziendale, prevalentemente confidenziale e sono visionabili solo dal destinatario di posta elettronica. La risposta o l'eventuale invio spontaneo da parte vostra di e-mail al nostro indirizzo potrebbero non assicurare la confidenzialità potendo essere viste da altri soggetti appartenenti alla Fondazione Teatro Massimo, oltre al sottoscritto, per finalità di sicurezza informatica, amministrative e allo scopo del continuo svolgimento dell'attività aziendale. Qualora questo messaggio vi fosse pervenuto per errore, vi preghiamo di cancellarlo dal vostro sistema e vi chiediamo di volercene dare cortesemente comunicazione."

3. È vietato creare, archiviare o spedire, anche solo all'interno della rete aziendale, messaggi pubblicitari o promozionali o comunque allegati (filmati, immagini, musica o altro) non connessi con lo svolgimento della propria attività lavorativa, nonché partecipare a richieste, petizioni, mailing di massa di qualunque contenuto, "catene di Sant'Antonio" o in genere a pubblici dibattiti utilizzando l'indirizzo aziendale.

4. È vietato trasmettere messaggi a gruppi numerosi di persone (es. a tutto un ufficio o ad un'intera divisione) senza l'autorizzazione necessaria e comunque, con gli indirizzi in chiaro di tutti i destinatari.

5. È vietato sollecitare donazioni di beneficenza, propaganda elettorale o altre voci non legate al lavoro.

	Documento gestione privacy Disposizione sull'uso di device, internet, posta elettronica ed archivi cartacei	01_02Disciplinare_uso_strumenti_inf ormatici		
		Rev.	Data	Foglio
		02	23/07/2025	11 di 16

6. È vietato utilizzare il servizio di posta elettronica per trasmettere a soggetti esterni dell'organizzazione informazioni riservate o comunque documenti aziendali, se non nel caso in cui ciò sia necessario in ragione delle mansioni svolte.

7. È vietato utilizzare la posta elettronica per messaggi con allegati di grandi dimensioni, a meno di preventiva autorizzazione da parte dell'amministratore di sistema.

Ed inoltre, si sottolinea:

1. È vietato inviare, tramite la posta elettronica, anche all'interno della rete aziendale, materiale a contenuto violento, sessuale o comunque offensivo dei principî di dignità personale, di libertà religiosa, di libertà sessuale o di manifestazione del pensiero, anche politico.
2. È vietato inviare messaggi di posta elettronica, anche all'interno della rete aziendale, che abbiano contenuti contrari a norme di legge ed a norme di tutela dell'ordine pubblico, rilevanti ai fini della realizzazione di una fattispecie di reato, o che siano in qualche modo discriminatori della razza, dell'origine etnica, del colore della pelle, della fede religiosa, dell'età, del sesso, della cittadinanza, dello stato civile, degli handicap.
3. Qualora l'Incaricato riceva messaggi aventi tale contenuto, è tenuto a cancellarli immediatamente e a darne comunicazione all'organizzazione.

Posta Elettronica in caso di assenze programmate, non programmate.

Nel caso di assenza prolungata sarà buona norma attivare il servizio di risposta automatica (Auto-reply). A tal fine, è cura dell'amministratore di sistema, mettere a disposizione dell'incaricato anche apposite funzionalità di sistema, di agevole utilizzo, che consentano di inviare automaticamente in caso di assenze (per es., per ferie o attività di lavoro fuori sede), messaggi di risposta contenenti le "coordinate" (anche elettroniche o telefoniche) di un altro soggetto o altre utili modalità di contatto dell'incaricato assente o della Fondazione Teatro Massimo.

In alternativa e in tutti i casi in cui sia necessario un presidio della casella di e-mail, per ragioni di operatività aziendale, l'Incaricato deve nominare un collega fiduciario con lettera scritta che in caso di assenza inoltri i files necessari a chi ne abbia urgenza.

Qualora l'Incaricato non abbia provveduto ad individuare un collega fiduciario o questi sia assente o irreperibile, la Fondazione Teatro Massimo, informerà preventivamente (e solo ove non sia possibile successivamente) l'incaricato stesso, spiegando modalità e motivazioni dell'intervento, che il contenuto dei messaggi di posta elettronica verrà verificato da un incaricato, temporaneamente, modificando le credenziali di accesso. Di tale attività sarà redatto apposito verbale.


L'eventuale controllo o il monitoraggio delle mail sarà sempre graduale, dovendosi così escludere l'ammissibilità di controlli prolungati, costanti o indiscriminati; sono comunque vietate la lettura e la registrazione sistematica dei messaggi di posta elettronica ovvero dei relativi dati esteriori, al di là di quanto tecnicamente necessario per svolgere il servizio e-mail.

Trattandosi poi di controlli a distanza sarà certamente applicabile la disciplina di cui all'art. 4 della legge 300/1970, in modo che la policy sia trasparente e condivisa tra la Fondazione Teatro Massimo e lavoratori.

Ogni forma di controllo occulto è vietata e comunque in Fondazione è vietato l'uso di "sniffer" o altri dispositivi hardware o software finalizzati all'intercettazione e/o all'interruzione e/o all'impedimento di comunicazioni telematiche, come quelle che avvengono tramite e-mail.

Posta Elettronica in caso di cessazione dell'incarico

In caso di cessazione per qualsivoglia ragione e/o causa del rapporto di lavoro e/o di collaborazione e/o altro in essere con la Fondazione Teatro Massimo, gli account riconducibili a persone identificate o

	Documento gestione privacy Disposizione sull'uso di device, internet, posta elettronica ed archivi cartacei	01_02Disciplinare_uso_strumenti_informatici		
		Rev.	Data	Foglio
		02	23/07/2025	12 di 16

identificabili saranno rimossi previa disattivazione degli stessi e contestuale adozione di sistemi automatici volti ad informarne i terzi ed a fornire a questi ultimi indirizzi alternativi riferiti all'attività professionale del titolare del trattamento. *(L'interesse della Fondazione Teatro Massimo ad accedere alle informazioni necessarie all'efficiente gestione della propria attività, pertanto, verrà temperato con la legittima aspettativa di riservatezza sulla corrispondenza da parte dei dipendenti nonché dei terzi).*

Le email precedentemente archiviate nell'account del dipendente o collaboratore cessato non potranno essere custodite, all'interno del server, per un periodo di tempo superiore a 3 mesi "fatta salva la conservazione per esclusiva finalità di tutela dei diritti in sede giudiziaria".

16. L'utilizzo del notebook, tablet o smartphone.

Il computer portatile, il tablet e il cellulare (di seguito generalizzati in "dispositivo mobile") possono venire concessi in uso dall'organizzazione agli Incaricati che durante gli spostamenti necessitano di disporre di archivi elettronici, supporti di automazione e/o di connessione alla rete dell'organizzazione.

L'Incaricato è responsabile dei dispositivi mobili assegnatigli dall'organizzazione e deve custodirli con diligenza sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro.

Ai dispositivi mobili si applicano le regole di utilizzo previste per i computer connessi in rete, con particolare attenzione alla rimozione di eventuali file elaborati sullo stesso prima della riconsegna. In particolare i files creati o modificati sui dispositivi mobili devono essere trasferiti sulle memorie di massa aziendali al primo rientro in ufficio e cancellati in modo definitivo dai dispositivi mobili.

Sui dispositivi mobili è vietato installare applicazioni (anche gratuite) se non espressamente autorizzate dalla direzione.

I dispositivi mobili utilizzati all'esterno, in caso di allontanamento, devono essere custoditi in un luogo protetto.

Anche di giorno, durante l'orario di lavoro, all'Incaricato non è consentito lasciare incustoditi i dispositivi mobili.

All'Incaricato è vietato lasciare i dispositivi mobili incustoditi e a vista dentro l'auto o in una stanza d'albergo o nell'atrio dell'albergo o nelle sale d'attesa delle stazioni ferroviarie e aeroportuali.

I dispositivi mobili che permettono l'attivazione di una procedura di protezione (PIN) devono sempre essere abilitabili solo con la digitazione del PIN stesso e non possono essere lasciati privi di PIN.


Laddove il dispositivo mobile sia accompagnato da un'utenza, l'Incaricato è chiamato ad informarsi preventivamente dei vincoli ad essa associati (es. numero minuti massimo, totale gigabyte dati, ...) e a rispettarli. Qualora esigenze lavorative richiedessero requirements differenti l'Incaricato è tenuto ad informare tempestivamente e preventivamente dalla Fondazione Teatro Massimo.

In relazione alle utenze mobili, salvo autorizzazione dell'organizzazione, è espressamente vietato ogni utilizzo all'estero e anche in caso di autorizzazione dell'organizzazione, gli utilizzi all'esterno devono essere preventivamente comunicati all'organizzazione per permettere l'attivazione di opportuni contratti di copertura con l'operatore mobile di riferimento.

17. Memorie esterne (chiavi usb, hard disk, memory card, cd-rom, dvd, ecc.)

Agli Incaricati può essere assegnata una memoria esterna (quale una chiave USB, un hard disk esterno, una memory card, ...) su cui copiare temporaneamente dei dati per un facile trasporto, o altri usi (es. macchine fotografiche con memory card, videocamere con dvd, ...).

Questi dispositivi devono essere gestiti con le stesse accortezze di cui all'articolo precedente e devono essere utilizzati esclusivamente dalle persone a cui sono state affidate e, in nessun caso, devono essere consegnate a terzi.

	Documento gestione privacy Disposizione sull'uso di device, internet, posta elettronica ed archivi cartacei	01_02Disciplinare_uso_strumenti_inf ormatici		
		Rev.	Data	Foglio
		02	23/07/2025	13 di 16

Distruzione dei Dispositivi

Ogni Dispositivo ed ogni memoria esterna affidati agli incaricati, (computer, notebook, tablet, smartphone, memory card, chiavi usb, hard disk, dvd, cd-rom, ecc.), al termine del loro utilizzo dovranno essere restituiti alla Fondazione Teatro Massimo che provvederà a distruggerli o a ricondizionarli seguendo le norme di legge in vigore al momento.

In particolare la Fondazione Teatro Massimo provvederà a cancellare o a rendere inintelligibili i dati negli stessi memorizzati.

18. Utilizzo del cellulare/smartphone personale.

Durante l'orario di lavoro, comprese le eventuali pause, agli Incaricati è concesso l'utilizzo del telefono cellulare personale ma solo per comunicazioni di emergenza o strettamente collegate all'ambito lavorativo.

In caso di trasferte lavorative all'esterno degli uffici dell'organizzazione, il telefono personale può rimanere acceso, anche per facilitare la comunicazione con l'organizzazione stessa ove fosse necessario.

In questo caso si invita, comunque, a non utilizzarlo per fini personali, in modo particolare alla presenza di clienti o fornitori.

Gli Incaricati non dipendenti (ovvero i consulenti e collaboratori esterni), possono utilizzare i propri cellulari/smartphone per memorizzare dati della Fondazione Teatro Massimo solo se espressamente autorizzati e assumendone formalmente e personalmente l'intera responsabilità del trattamento.

Tali cellulari/smartphone dovranno essere preventivamente valutati dall'amministratore di sistema, per la verifica della sussistenza di misure minime ed idonee di sicurezza.

19. Utilizzo di sistemi cloud

L'utilizzo dei sistemi cloud (Drop box, Google drive, ...) deve essere approvato dalla Fondazione Teatro Massimo.

Per essere approvati i sistemi cloud devono rispondere ad almeno i seguenti requisiti:

- Essere sistemi cloud esclusivi e non condivisi;
- Essere sistemi cloud posizionati fisicamente in Italia;
- L'azienda che fornisce il sistema in cloud deve essere preventivamente nominata Responsabile al Trattamento dei dati da parte della Fondazione Teatro Massimo;
- L'azienda che fornisce il sistema in cloud deve comunicare alla Fondazione Teatro Massimo, almeno una volta all'anno, i nominativi degli amministratori di sistema utilizzati.
- Dovranno essere verificate tutte le indicazioni e prescrizioni previste dal Garante della Privacy nei suoi provvedimenti sugli Amministratori di Sistema e sul cloud.


20. Organizzazione della scrivania

Gli Incaricati sono responsabili del controllo e della custodia, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, degli atti e dei documenti contenenti dati personali.

Gli Incaricati sono invitati dall'organizzazione ad adottare una "politica della scrivania pulita". Ovvero si richiede agli incaricati di trattare dati cartacei solo se necessario, privilegiando, ove possibile, l'utilizzo degli strumenti digitali messi a disposizione dalla Fondazione Teatro Massimo.

I principali benefici di una politica della scrivania pulita sono:

- 1) Una buona impressione a clienti e fornitori che visitano la nostra Fondazione;
- 2) La riduzione della possibilità che informazioni confidenziali possano essere viste da persone non abilitate a conoscerle;
- 3) La riduzione che documenti confidenziali possano essere sottratti all'organizzazione.

	Documento gestione privacy Disposizione sull'uso di device, internet, posta elettronica ed archivi cartacei	01_02Disciplinare_uso_strumenti_informatici		
		Rev.	Data	Foglio
		02	23/07/2025	14 di 16

In particolare, si invita a non lasciare in vista sulla propria scrivania dati cartacei quando ci si allontana dalla stessa oppure quando è previsto un incontro con un soggetto non abilitato alla conoscenza dei dati in essi contenuti.

Prima di lasciare la propria postazione (per esempio per la pausa pranzo o per una riunione) sarà cura degli Incaricati riporre in luogo sicuro (armadio, cassettera, archivio, ...) i dati cartacei ad esso affidati, affinché gli stessi non possano essere visti da terzi non autorizzati (es. addetti alle pulizie) o da terzi (visitatori) presenti in sede.

A fine giornata deve essere previsto il riordino della scrivania e la corretta archiviazione di tutte le pratiche d'ufficio, in modo da lasciare la scrivania completamente sgombra.

Ove possibile, si invita ad evitare la stampa di documenti digitali, anche ai fini di ridurre l'inquinamento ed il consumo delle risorse in ottica ecologica.

Ove possibile, si invita ad effettuare la scansione dei documenti cartacei ed archivarli digitalmente.

È necessario rimuovere immediatamente ogni foglio stampato da una stampante o da un'apparecchiatura fax, per evitare che siano prelevati o visionati da soggetti non autorizzati.

Ove possibile, è buona norma eliminare i documenti cartacei attraverso apparecchiature trita documenti.

21. In caso di furto

In caso di perdita o furto dei dispositivi consegnati e/o di documentazione aziendale, sarà obbligo dell'incaricato comunicare via mail a privacy@teatromassimo.it, tempestivamente al momento della scoperta, l'accaduto, circostanziando il fatto dettagliatamente, in modo che la Fondazione possa procedere con le denunce del caso e l'attuazione delle contromisure ritenute opportune.

22. Controlli

La Fondazione Teatro Massimo, in qualità di Titolare degli strumenti informatici, dei dati ivi contenuti e/o trattati, si riserva la facoltà di effettuare i controlli che ritiene opportuni per le seguenti finalità:

1. Tutelare la sicurezza e preservare l'integrità degli strumenti informatici e dei dati.
2. Evitare la commissione di illeciti o per esigenze di carattere difensivo anche preventivo.
3. Verificare la funzionalità del sistema e degli strumenti informatici.
4. Analizzare le dinamiche di un'eventuale compromissione dati "Data Breach".

Le attività di controllo potranno avvenire in modo logic anche con audit del sistema informatico. Per tali controlli l'organizzazione si riserva di avvalersi di soggetti esterni.


Si precisa, in ogni caso, che l'organizzazione non adotta "apparecchiature per finalità di controllo a distanza dell'attività dei lavoratori" (ex art. 4, primo comma, l. n. 300/1970), tra cui sono certamente comprese le strumentazioni hardware e software mirate al controllo dell'utente.

23. Modalità di verifica

La Fondazione Teatro Massimo promuove ogni opportuna misura, organizzativa e tecnologica volta a prevenire il rischio di utilizzi impropri e, comunque, a "minimizzare" l'uso di dati riferibili agli Incaricati e allo scopo ha adottato ogni possibile strumento tecnico, organizzativo e fisico, volto a prevenire trattamenti illeciti sui dati trattati con strumenti informatici.

La Fondazione Teatro Massimo informa di non adottare sistemi che determinano interferenza ingiustificata sui diritti e sulle libertà fondamentali di lavoratori, come pure di soggetti esterni che ricevono o inviano comunicazioni elettroniche di natura personale o privata.

In particolare eventuali sistemi atti a monitorare eventuali violazioni di legge o comportamenti anomali da parte degli Incaricati avvengono nel rispetto del principio di pertinenza e non eccedenza, con esclusione di registrazioni o verifiche con modalità sistematiche.

	Documento gestione privacy Disposizione sull'uso di device, internet, posta elettronica ed archivi cartacei	01_02Disciplinare_uso_strumenti_inf ormatici		
		Rev.	Data	Foglio
		02	23/07/2025	15 di 16

Qualora nell'ambito di tali verifiche si dovesse rilevare un evento dannoso, una situazione di pericolo o qualche altra modalità non conforme all'attività lavorativa (es. scarico di files pirata, navigazioni da cui sia derivato il download di virus informatici, ecc.):

- si effettuerà un avvertimento in modo generalizzato con l'invito ad attenersi scrupolosamente ai compiti assegnati e alle istruzioni impartite;
- si procederà ad effettuare controlli più mirati che coinvolgano i dipendenti afferenti all'area o al settore in cui è stata rilevata l'anomalia.

24. Modalità di Conservazione

I sistemi software sono stati programmati e configurati in modo da cancellare periodicamente ed automaticamente i dati personali relativi agli accessi ad Internet e al traffico telematico, la cui conservazione non sia necessaria.

Un eventuale prolungamento dei tempi di conservazione viene valutato come eccezionale e deve aver luogo solo in relazione:

1. Ad esigenze tecniche o di sicurezza del tutto particolari;
2. All'indispensabilità del dato rispetto all'esercizio o alla difesa di un diritto in sede giudiziaria;
3. All'obbligo di custodire o consegnare i dati per ottemperare ad una specifica richiesta dell'autorità giudiziaria o della polizia giudiziaria.

In questi casi, il trattamento dei dati personali è limitato alle sole informazioni indispensabili per perseguire finalità preventivamente determinate ed essere effettuato con logiche e forme di organizzazione strettamente correlate agli obblighi, compiti e finalità già esplicitati.

25. Segreto aziendale

Il dipendente o collaboratore non può divulgare, pubblicare o comunicare in alcun modo a terzi, direttamente o indirettamente, in toto o in parte, le informazioni apprese in occasione dello svolgimento delle mansioni per le quali è stato assunto dalla Società, né potrà usarle, sfruttarle o disporne in proprio o tramite terzi.

Gli obblighi del dipendente o collaboratore previsti in questo capo non termineranno all'atto di cessazione del rapporto di lavoro, se non in riferimento a quelle specifiche parti delle informazioni che il dipendente o collaboratore possa dimostrare che erano già di pubblico dominio al momento della conclusione del rapporto, o che lo sono diventate in seguito per fatto a lui non imputabile.

26. Individuazione dei Soggetti autorizzati


La Fondazione Teatro Massimo ha designato un amministratore di sistema cui impartire precise istruzioni sul tipo di controlli ammessi e sulle relative modalità.

Per quanto riguarda i soggetti preposti al connesso trattamento dei dati (in particolare, gli incaricati della manutenzione) sono stati appositamente incaricati di svolgere solo operazioni strettamente necessarie al perseguimento delle finalità di sicurezza informatica, senza realizzare attività di controllo a distanza, neanche di propria iniziativa.

I soggetti che operano quali amministratori di sistema o le figure analoghe cui siano rimesse operazioni connesse al regolare funzionamento dei sistemi, svolgono un'attività formativa sui profili tecnico-gestionali e di sicurezza delle reti, sui principi di protezione dei dati personali e sul segreto nelle comunicazioni.

27. Conseguenze delle infrazioni disciplinari

Nel momento in cui il dipendente non rispetti gli obblighi del presente disciplinare, conformemente a quanto disposto dal CCNL, la sua condotta potrà essere soggetta a procedimento disciplinare.

	Documento gestione privacy Disposizione sull'uso di device, internet, posta elettronica ed archivi cartacei	01_02Disciplinare_uso_strumenti_informatici		
		Rev.	Data	Foglio
		02	23/07/2025	16 di 16

Sulla base della gravità dell'infrazione commessa, il dipendente può andare incontro a:

- Rimprovero verbale
- Rimprovero scritto
- Multa non superiore a 3 ore di stipendio
- Sospensione dal lavoro, o dallo stipendio e dal lavoro, per un periodo fino a 5 giorni
- Sospensione dallo stipendio e dal lavoro per un periodo non superiore a 10 giorni
- Licenziamento senza preavviso e con la perdita della relativa indennità

28. Modalità di Esercizio dei diritti

Il lavoratore interessato del trattamento dei dati effettuato mediante strumenti informatici ha diritto di accedere ai sensi del Capo III del GDPR alle informazioni che lo riguardano scrivendo all'indirizzo pec ergon.serviziodpo@pec.it oppure all'indirizzo di posta elettronica privacy@teatromassimo.it.

29. Validità, aggiornamento e diffusione

Il presente Disciplinare ha validità a partire dal 23/07/2025

Il presente Disciplinare sarà oggetto di aggiornamento ogni volta che se ne ravvisi la necessità, in caso di variazioni tecniche dei sistemi della Fondazione o in caso di mutazioni legislative. Ogni variazione del presente Disciplinare sarà comunicata agli incaricati.

Il presente Disciplinare verrà pubblicato sul nostro sito web e sull'App ZConnect ai sensi dell'art. 7 della legge 300/70 e del CCNL.

Data 23/07/2025

Firma
 Titolare del trattamento dei dati
 Fondazione Teatro Massimo