Liceo Ariosto-Spallanzani

LOGO

ISTRUZIONI OPERATIVE PER LE PERSONE AUTORIZZATE A TRATTARE I DATI PERSONALI

ai sensi del Regolamento UE 2016/679

"General Data Protection Regulation"

Data	Redatto da:	Verificato da:	Approvato da:
25/01/2023	**Laura Menozzi** **Data Protection Officer**	**Nome ADS**	_____

Sommario

1. Finalità

Il presente documento ha la finalità di regolamentare l'utilizzo degli Strumenti Informatici utilizzati dall'Istituto **Liceo Ariosto-Spallanzani**, sia aziendali forniti dal Titolare stesso che personali, di cui sia stato autorizzato l'uso a scopo lavorativo.

Ciò allo scopo preciso di istruire il personale circa il corretto uso degli strumenti IT ed evitare così i rischi conseguenti da uno scorretto o illecito utilizzo di tali strumenti sia all'interno dell'Azienda che all'esterno, comunque nello svolgimento dell'attività lavorativa, salvaguardando in tal modo i dati degli stessi soggetti incaricati, dell'Ente titolare e di coloro che intrattengano con essa rapporti di collaborazione e/o commerciali.

La diligenza, la buona fede e la correttezza devono quindi essere i principi sui quali basare l'utilizzo degli Strumenti Aziendali e degli Strumenti Personali da parte della Persone Autorizzate.

Il presente documento, che nei successivi paragrafi contiene precise regole di comportamento, **deve quindi essere letto, compreso e applicato** da tutti i soggetti autorizzati.

Si specifica che Istituto **Liceo Ariosto-Spallanzani** non attuerà alcuna politica di controllo o indagine, anche a distanza, delle attività dei soggetti autorizzati, in conformità con quanto previsto dagli artt. 4 e 8 dello Statuto dei Lavoratori (Legge 20 maggio 1970 n. 300).

I controlli saranno volti esclusivamente a verificare il rispetto delle norme di seguito indicate e saranno svolti in conformità alla legge, in modo occasionale e saltuario, esclusivamente per eseguire verifiche sulla funzionalità e sicurezza del sistema, e per verificare la salvaguardia del patrimonio dell'Ente mediante il corretto utilizzo da parte dei dipendenti e collaboratori degli strumenti IT.

Nell'esercizio del potere di controllo ***il Titolare*** si atterranno al principio generale di proporzionalità e non eccedenza delle attività di controllo, rispettando le procedure di informazione/consultazione delle rappresentanze dei lavoratori previste dai contratti collettivi e informerà preventivamente i lavoratori dell'esistenza di dispositivi di controllo atti a raccogliere i dati personali.

2. Campo di applicazione

Per strumenti aziendali si intendono:

- ✓ Personal Computer Fisso;
- ✓ Personal Computer portatile;
- ✓ Rete Aziendale (LAN, Wi-fi, VPN, Intranet);
- ✓ Supporti Hardware (chiavette USB, Hard disk, Cd, memory card ecc..);
- ✓ Software licenziati;
- ✓ Server fisici;
- ✓ Server virtuali;
- ✓ Caselle di posta elettronica;
- ✓ Spazi Cloud (One Drive, Dropbox, Google Drive, e altri privati);
- ✓ Altri dispositivi di registrazione/archiviazione Dati;

La regolamentazione prevede, in generale, le seguenti disposizioni:

- Gli strumenti devono essere utilizzati e custoditi con cura, evitando qualsiasi danneggiamento, anche durante eventuali spostamenti.
- In caso di furto, smarrimento o danneggiamento dello strumento, è necessario che il fatto venga prontamente segnalato all'Ente, per fare in modo che venga dato corso alle azioni necessarie (denuncia presso le Autorità Pubbliche competenti ecc.) e che si proceda con le attività previste in caso di Data Breach.
- Gli strumenti devono essere utilizzati per scopi esclusivamente professionali, in relazione al ruolo/mansione, evitando l'uso promiscuo o illecito e la conservazione di dati personali.
- È vietato installare e utilizzare programmi non distribuiti dall'Ente o non attinenti l'attività lavorativa.

È vietato effettuare copia di dati personali e/o informazioni riservate e/o files appartenenti all'Istituto **Liceo Ariosto-Spallanzani** che siano disponibili per lo svolgimento della propria mansione lavorativa, per trasferirle a terzi o per farne un uso diverso da quello lavorativo.

3. Introduzione

Nell'espletamento delle sue attività lavorative le potrà essere assegnato uno o più dispositivi elettronici: ad esempio PC (mobile o fisso). Le seguenti istruzioni e regole dovranno essere seguite per un utilizzo corretto del dispositivo e conforme al GDPR.

I dispositivi assegnati per lo svolgimento dell'attività lavorativa non potranno **essere utilizzati per finalità personali né si potranno salvare documenti o file personali sui dispositivi**. Si ricorda che, per urgenze o particolari esigenze, il tecnico IT dell'Istituto **Liceo Ariosto-Spallanzani** potrebbe accedere ai dispositivi (in caso, ad esempio, di guasto) e potrebbero avere accesso ai suddetti dati. Per tali ragioni il salvataggio di file e documenti personali sui dispositivi aziendali è vietato e sotto la sua piena responsabilità.

Istruzioni e regole per il trattamento di dati con l'ausilio di strumenti elettronici

L'accesso a un qualunque tipo di strumenti elettronico è sempre subordinato al superamento di una procedura di autenticazione informatica che potrebbe prevedere l'inserimento da parte sua di un codice di identificazione (username) e di una parola chiave (password) riservata e conosciuta solamente da lei.

La parola chiave (password) rappresenta la prima barriera in una strategia di accesso selettivo a dati personali. Per queste ragioni ciascuno **è responsabile della segretezza della parola chiave associata al proprio codice di identificazione e tenuto a prendere tutte le iniziative appropriate per garantire la sicurezza della stessa**. Al primo ingresso le verrà assegnata una password provvisoria che dovrà provvedere a modificare al primo accesso e a consegnare in busta chiusa presso ……..

4. Istruzioni e raccomandazioni per la protezione della parola chiave

Non utilizzare la stessa parola chiave per sistemi di autenticazione interni e per sistemi di autenticazione esterni alla rete informatica del **Titolare**, come ad esempio l'accesso al proprio conto corrente bancario ed altre attività non legate all'attività lavorativa.

La parola chiave prescelta non deve essere condivisa con alcun soggetto ivi inclusi i superiori, a qualsiasi livello.

Di seguito un elenco degli accorgimenti da adottare:

- non rivelate una parola chiave attraverso il telefono a chicchessia
- non scrivete la parola chiave su un qualsiasi documento e non nascondetelo in alcuna parte del vostro ufficio
- non archiviate la parola chiave in chiaro in un qualsiasi tipo di sistema di elaborazione, incluso uno smartphone
- non rivelate la parola chiave al vostro superiore
- non parlate di parole chiave di fronte a terzi
- non date alcuna indicazione in merito al formato ed alla lunghezza della parola chiave, che utilizzate
- non svelate la parola chiave su questionari o su formulari di sicurezza
- non rivelate la parola chiave ad un vostro collega di lavoro
- non utilizzare mai la caratteristica, offerta da parecchie applicazioni, di memorizzare la parola chiave, piuttosto utilizzare un password manager.

Nel caso di operazioni sistemistiche che richiedano la vostra password (es: cambio del PC o installazione di programmi), il Tecnico IT la cambierà, dandovene comunicazione. Al primo utilizzo del PC è obbligatorio che modifichiate subito la password.

Per le credenziali di autenticazione personale di accesso al server è stata impostata una scadenza automatica al termine della quale, l'utente dovrà cambiarla e consegnarla in busta chiusa al referente IT che provvederà a custodirla in luogo idoneo e sottochiave. Sono state impostate delle credenziali di autenticazione anche per i PC portatili assegnati ai docenti. Sarà cura di ciascun utente modificare periodicamente (almeno una volta all'anno) tali credenziali. Per le LIM utilizzate nelle singole aule, invece, la password di accesso è unica per chiunque faccia l'accesso.

Se qualcuno insiste per conoscere la vostra parola chiave, dapprima fate riferimento a questo documento e successivamente informate immediatamente il **Responsabile di Area**.

Se avete anche solo il minimo sospetto che la vostra parola chiave sia stata in qualche modo compromessa o venuta a conoscenza di terzi, provvedete immediatamente alla sostituzione della

parola chiave e riferite l'accaduto al **Responsabile IT** e, nel caso in cui avete il minimo sospetto di una perdita di dati.

5. Istruzioni per la corretta creazione di una parola chiave

Parole chiave sicure

Sono da ritenere parole chiave di soddisfacente sicurezza quelle che hanno le seguenti caratteristiche:

- non devono rappresentare una parola in una qualsiasi lingua o dialetto sufficientemente diffuso
- non devono essere basate su informazioni personali, come nomi di membri della famiglia, date di nascita, anagrammi o combinazione di nomi e simili

Ecco qualche indicazione per creare delle parole chiave sicure ma facili da ricordare:

- creare una parola chiave, basata sul titolo di una canzone o su un'altra frase, debitamente sintetizzata - ad esempio "7000 caffè di Alex Britti" diventa "7000cffAB"
- la parola chiave può essere formata abbreviando una intera frase come ad esempio "Chi fa da se fa per 3!" diventa "Cfdsfx3!".

Attenzione: non usare mai gli esempi sopra illustrati come parola chiave

Parole chiave deboli

Si sottolinea che le parole chiave di facile individuazione hanno le seguenti caratteristiche:

- la parola chiave si può trovare in un comune dizionario italiano, in inglese od altra lingua comune
- la parola chiave è una parola di uso comune, come ad esempio il nome di qualche membro della famiglia, di animali da salotto, di amici, di collaboratori o di personaggi di fantasia
- sono da ritenere insoddisfacenti anche parole chiave legate a espressioni informatiche, hardware e software, come pure quelle legate a date di nascita od altre informazioni personali, come l'indirizzo, il numero telefonico e simili
- è da scartare una qualsiasi delle parole chiave precedentemente indicata come debole, preceduta o seguita da una cifra come ad esempio Giovanni1, oppure 1Giovanni.

6. Istruzioni per l'utilizzo della casella di posta elettronica aziendale

Ad ogni nuova assunzione/collaborazione il tecnico IT provvederà a creare un suo specifico account di posta elettronica con credenziali che lei dovrà modificare al primo accesso con criteri che rispettano i criteri di sicurezza di cui sopra.

La casella di posta elettronica è uno strumento di lavoro, per cui deve essere utilizzata per attività esclusivamente lavorative e lei è responsabile del suo corretto utilizzo, è **vietato quindi l'utilizzo promiscuo della posta elettronica per scopi sia aziendali che personali**.

Allo scopo di garantire la funzionalità del servizio di posta elettronica e i rapporti commerciali, **in caso di assenza prolungata programmata** (ad es. ferie) lei dovrà predisporre un messaggio automatico di risposta (**auto-reply**) avvisando dell'assenza e fino a quale giorno, indicando un indirizzo di posta elettronica alternativo con relativo referente a cui l'utente potrà inviare il proprio messaggio in caso di necessità.

In caso di assenza improvvisa non programmata (ad es. malattia), sarà cura del tecnico IT accedere alla sua casella di posta elettronica al fine di impostare l'auto-reply.

È necessario inoltre ricordare che l'utilizzo dell'e-mail può comportare dei rischi derivanti dalla possibile intercettazione della medesima e, quindi, i documenti in essa contenuti potrebbero essere letti e/o utilizzati da persone non autorizzate al trattamento.

È necessario, inoltre, prestare molta attenzione alle e-mail che giungono nella propria casella di posta, in quanto queste potrebbero essere state inviate in automatico da sistemi infetti da virus e quindi potrebbero contenere esse stesse dei virus. **Qualora giungessero e-mail da mittenti sconosciuti evitare, in prima analisi, di aprire eventuali allegati**.

Importante ricordare che, nei casi di inoltro di e-mail a più destinatari esterni al **Titolare** che non hanno l'esigenza di conoscere gli altri destinatari, occorre utilizzare la funzionalità di invio per conoscenza nascosta (Ccn).

7. Istruzioni e raccomandazioni per la rilevazione e protezione dalle minacce di phishing

Il phishing è un'azione volta al furto dell'identità informatica, cioè di quelle informazioni, generalmente riservate, che permettono di identificare un soggetto che accede ad un sistema informatico (es. le credenziali di accesso al pc, le credenziali di accesso al portale internet del conto corrente bancario, ecc.).

Il phishing inizia con la ricezione di una e-mail inviata dal truffatore alle potenziali vittime. Di norma il messaggio di posta ha un aspetto formale e cerca di indurre il destinatario ad effettuare una serie di operazioni abbastanza usuali per coloro che usufruiscono dei servizi web on-line.

Ad esempio l'invito a "cliccare" sull'indirizzo del sito (in questo caso pirata) e la presentazione di una pagina web che appare con tutte le caratteristiche dell'azienda con la quale l'utente ha stipulato il servizio on-line. Se la vittima inserisce i propri dati tramite l'apposita pagina web, scatta il meccanismo di raccolta delle informazioni che, una volta in possesso del truffatore, possono essere usate in modo fraudolento.

Si riporta un esempio di e-mail phishing.

"*Gentile Cliente,*

questa e-mail Le è stata inviata dai server di (di solito il nome di una banca) per evitare che il suo account (nome utente e password) sia disattivato per inutilizzo. Per completare l'operazione è sufficiente che Lei faccia click sul link seguente ed effettui il log-in come di consueto. Tutto questo per garantire la protezione dei suoi dati. Infatti è stato riscontrato che molti utenti non effettuano l'accesso da tanto tempo. Per verificare il suo account faccia click sul link seguente e, quindi, effettui il log-in come di consueto: www.nomebanca.com/verificaaccount "

Per scongiurare le minacce di phishing è utile attenersi ai seguenti punti:

- evitare di rispondere a richieste di informazioni personali ricevute tramite posta elettronica, se non si ha certezza della provenienza. Nel dubbio, è sempre preferibile verificare l'attendibilità dell'informazione o della richiesta contattando il mittente con canali diversi (es. telefono).
- anche se il link nella e-mail o la barra degli indirizzi web risulta (apparentemente) corretto, è bene sapere che esistono delle tecniche, usate dagli hacker, per mascherare l'indirizzo fasullo con uno corretto. Se c'è il minimo sospetto è meglio fare una segnalazione all'ICT ed evitare di "cliccare" sui link per accedere ai relativi siti web. Questi collegamenti potrebbero condurre al sito pirata. Invece, aprire una nuova finestra del browser e digitare a mano l'indirizzo.
- i siti legittimi che richiedono informazioni riservate codificano (criptano) sempre la sessione. Quindi accertarsi sempre che il sito web che richiede i dati, adotti dei validi sistemi di crittografia, per esempio SSL - Secure Sockets Layer, verificando la presenza dell'icona del lucchetto sulla parte in alto a sinistra del browser. Fare doppio click sul lucchetto per verificare il certificato SSL.

8. Istruzioni e raccomandazioni per la rilevazione e protezione dalle minacce di pharming

Il pharming è un'estensione estremamente sofisticata del phishing. A differenza di quest'ultimo, gli attacchi di Pharming rimangono nascosti in un computer connesso alla rete e raccolgono informazioni sui dati finanziari durante la normale navigazione delle vittime. Gli utenti che vogliono collegarsi a un sito web sono, a loro insaputa, dirottati verso un sito artefatto simile a quello originale. Una volta impiantato lo schema di pharming, può partire l'attività dannosa contro un gran numero di siti che l'utente visita regolarmente, senza che la vittima se ne renda minimamente conto.

Per identificare le minacce di pharming è utile sapere che:

- i processi di login, verifica o informazione mostrati nei siti pirata non sono esattamente identici a quelli del sito autentico
- è probabile che i siti di pharming richiedano informazioni di verifica o personali che solitamente non sono necessarie

- i siti legittimi che richiedono informazioni riservate codificano (criptano) sempre la sessione. Quindi accertarsi sempre che il sito web che richiede i dati, adotti dei validi sistemi di crittografia, per esempio SSL - Secure Sockets Layer, verificando la presenza dell'icona del lucchetto sulla parte in alto a sinistra del browser. Fare doppio click sul lucchetto per verificare il certificato SSL
- in un sito sicuro, l'indirizzo (URL) che compare nel browser dovrebbe contenere il prefisso https:// nella barra dell'indirizzo. I siti di pharming generalmente non hanno certificati SSL per cui il prefisso http:// rimane anche quando si devono inserire dati riservati
- se il browser rileva l'esistenza di un problema con il certificato SSL, invece di ignorarlo, gli utenti devono cogliere l'occasione per controllare il certificato e considerarlo come un segno evidente di sito fraudolento.

9. Ulteriori policy di autenticazione per dispositivi mobili

Per l'utilizzo e l'accesso ai dispositivi mobili aziendali (PC portatili) è obbligatorio attivare un sistema di autenticazione con password alfanumerica

Tali strumenti dovranno essere utilizzati solo ed esclusivamente per finalità lavorative. Qualunque comunicazione, file o contenuto digitale di tipo personale non deve essere salvato sul dispositivo.

In caso di furto o smarrimento del dispositivo occorre informare tempestivamente il responsabile di riferimento per poter attivare la procedura di gestione del data breach.

10. Accesso ai dati ad opera del Titolare in caso di emergenza

Si informa che il **Titolare** è tenuto ad adottare idonee e preventive procedure che consentano l'accesso ai dati e ai sistemi, protetti dalla componente riservata delle credenziali (password), in caso di sua prolungata assenza o impedimento e in caso si renda necessario e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema.

Resta inteso che dal momento in cui, per l'accesso ai dati in caso di emergenza, il **Titolare** o il Tecnico IT dovessero procedere ad aprire la busta contenente la sua password d'accesso, gliene verrà data pronta comunicazione. Terminata la fase di emergenza, prima di riutilizzare nuovamente lo strumento dovrà impostare una nuova parola chiave.

11. Disattivazione delle credenziali di accesso

Si sottolinea che per motivi di sicurezza le credenziali di accesso saranno disattivate in caso di:

- perdita del diritto di accesso ai dati per qualunque motivo
- accesso in caso di emergenza ad opera del **Titolare**

Qualora ci si trovasse nella impossibilità ad accedere al sistema con le credenziali assegnate occorre rivolgersi al Responsabile di riferimento.

- Nel caso di perdita del diritto di accesso, come ad esempio per cessazione del rapporto lavorativo, le sue credenziali saranno disattivate e la sua casella di posta elettronica sarà cancellata.

12. Sessioni di trattamento dati incustodite

Si raccomanda di non lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento di dati personali, in particolare qualora sia necessario allontanarsi temporaneamente dal posto di lavoro. Si ricorda che la pressione contemporanea dei tasti Ctrl + Alt + Canc attiva la finestra di "Protezione di Windows" dalla quale è possibile premere il pulsante "Blocca computer" per bloccare la stazione di lavoro senza la necessità di uscire dai programmi in uso. Una volta ritornati davanti alla propria postazione, per riprendere l'operatività è necessario seguire le istruzioni a video delle finestre di Windows premendo nuovamente i tasti Ctrl + Alt + Canc e inserendo la propria password.

Per cautelarsi ulteriormente dalle eventualità di lasciare sessioni di trattamento di dati personali incustodite, lei potrà impostare un blocco automatico della propria postazione di lavoro che richieda l'inserimento della password in fase di ripristino. Per far ciò è necessario eseguire le operazioni specifiche per ogni sistema operativo. Rivolgersi al proprio servizio IT per un supporto specifico.

Il blocco automatico con password è da considerarsi, comunque, una misura atta a ridurre, e non ad eliminare a causa del suo ritardo di attivazione, possibili rischi di trattamento dati da parte di persone non autorizzate. Lei dovrà pertanto prendere tutte le cautele affinché ciò non avvenga, ad esempio mediante il blocco della stazione di lavoro nella modalità manuale sopra identificata.

13. Istruzioni e raccomandazioni per l'organizzazione dei dati su File System

Si ricorda che le uniche aree autorizzate al salvataggio di dati sono gli spazi riservati sul server.

Tali spazi sono configurati al fine di garantire la sicurezza e la custodia dei dati in conformità a quanto previsto dal profilo di incarico assegnato, impedendo accessi non consentiti, assicurando disponibilità dei dati in caso di emergenza e sottoposti a backup in conformità a quanto previsto dal GDPR.

Qualora, accedendo al server, lei si accorga di:

- aver involontariamente cancellato un file
- aver involontariamente corrotto un file
- non reperire il file che si vuole aprire

è necessario che si rivolga al Tecnico IT.

Se invece si utilizzano supporti rimovibili (cd-rom, chiavi USB…) per il trasferimento e la modifica di file, occorre mantenerne una copia aggiornata sul server della rete informatica della Società.

Se per ragioni di lavoro si è costretti a lavorare in spazi diversi dal server si ricorda l'obbligo di **riversare, appena possibile, i file lavorati sulle aree del server**, per poter sottoporli a backup.

14. Istruzioni e raccomandazioni per l'utilizzo di hardware e software

Il software installato in ciascuna macchina (sistema operativo, Office Automation…) nonché le relative configurazioni hardware, rispecchiano la condizione necessaria e sufficiente per il consueto lavoro da svolgersi e comunque valutato e stabilito dal **Titolare**.

Qualora riteniate necessario disporre di un nuovo software o di un aggiornamento hardware per le consuete mansioni, è **proibito procedere all'auto-installazione** dei medesimi ma è necessario informare il Tecnico IT che valuterà l'opportunità dell'upgrade della macchina.

È bene ricordare che ogni software ha una licenza e l'uso improprio di questa può portare a conseguenze civili.

Inoltre agli utenti dei Personal Computer non è consentito l'accesso ai parametri di configurazione dei software e del Sistema Operativo, per modificare i quali è sempre necessaria una specifica attività da parte degli Amministratori di Sistema.

15. Navigazione in Internet

L'Ente ha definito una black list pertanto il singolo utente non è abilitato alla libera navigazione in Internet. L'accesso al web costituisce comunque uno strumento aziendale utilizzabile esclusivamente per lo svolgimento della propria attività lavorativa. È quindi assolutamente proibita la navigazione in Internet per motivi diversi da quelli strettamente legati all'attività lavorativa.

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

- l'upload o il download di software anche gratuiti (freeware) e shareware, nonché l'utilizzo di documenti provenienti da siti web o http, se non strettamente attinenti all'attività lavorativa (filmati e musica) e previa verifica dell'attendibilità dei siti in questione (nel caso di dubbio, dovrà venir a tal fine contattato il personale del Servizio ICT);
- l'effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti on-line e simili, fatti salvi i casi direttamente autorizzati dalla Direzione Generale (o eventualmente dal Responsabile d'ufficio e/o del Servizio ICT) e comunque nel rispetto delle normali procedure di acquisto;
- ogni forma di registrazione a siti i cui contenuti non siano strettamente legati all'attività lavorativa;
- la partecipazione a Forum non professionali, l'iscrizione con account aziendale e la partecipazione personale a social network, l'utilizzo di chat line (esclusi gli strumenti autorizzati), di bacheche elettroniche e le registrazioni in guest books anche utilizzando pseudonimi (o nicknames) se non espressamente autorizzati dal Responsabile d'ufficio;

Potranno essere svolti ,dal personale incaricato, eventuali controlli sui "file di log" della navigazione svolta. Tale controllo sui file di log non è continuativo ed i file stessi vengono conservati non oltre sei mesi, ossia il tempo indispensabile per il corretto perseguimento delle finalità organizzative e di sicurezza dell'Azienda.

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

L'accesso da remoto alla rete aziendale è possibile agli utenti abilitati solo a seguito di comunicazione di specifiche credenziali o dell'installazione di software che lo abilita sui dispositivi in uso.

16.Protezione antivirus

Il sistema informatico dell'Istituto **Liceo Ariosto-Spallanzani** è protetto da antivirus e Endian firewall. Ogni utente deve comunque tenere comportamenti tali da ridurre il rischio di attacco al sistema informatico aziendale mediante virus o mediante ogni altro software aggressivo.

Nel caso il software antivirus rilevi la presenza di un virus, l'utente dovrà immediatamente sospendere ogni elaborazione in corso senza spegnere il computer nonché segnalare prontamente l'accaduto al personale del Servizio ICT. Anche in caso di ricezione di mail sospette occorre segnalarle all'ICT prima di scaricare/aprire qualsiasi allegato o link presente nella stessa.

17. Partecipazioni a social media

L'utilizzo dei social media – quali Facebook, Twitter, Linkedin, dei blog e dei forum, anche professionali – verrà gestito ed organizzato esclusivamente dall'Ente attraverso specifiche direttive ed istruzioni operative al personale a ciò espressamente addetto, rimanendo escluse iniziative individuali da parte dei singoli utenti

Fermo restando il pieno ed inderogabile diritto della persona alla libertà di espressione ed al libero scambio di idee ed opinioni, l'Ente ritiene comunque opportuno indicare agli utenti alcune regole comportamentali, al fine di tutelare tanto la propria immagine ed il patrimonio dell'Ente, anche immateriale, quanto i propri collaboratori, i propri alunni, fornitori, gli altri partners, oltre che gli stessi utenti utilizzatori dei social media, fermo restando che viene vietata la partecipazione agli stessi social media durante l'orario di lavoro. La policy qui dettata deve venir seguita dagli utenti sia che utilizzino dispositivi messi a disposizione dall'Ente, sia che utilizzino propri dispositivi, sia che partecipino ai social media a titolo personale, sia che lo facciano per finalità professionali, come dipendenti della stesso Ente.

La condivisione dei contenuti nei social media deve sempre rispettare e garantire la segretezza sulle informazioni considerate dall' Ente riservate ed in genere. Inoltre, ogni comunicazione e divulgazione di contenuti dovrà essere effettuata nel pieno rispetto dei diritti di proprietà e dei diritti d'autore, sia di terzi che dell' Ente.

L'utente deve garantire la tutela della privacy delle persone; di conseguenza, non potrà comunicare o diffondere dati personali (quali dati anagrafici, immagini, video, suoni e voci) di colleghi e in genere di collaboratori aziendali, se non con il preventivo personale consenso di questi, e comunque non

potrà postare nel social media immagini, video, suoni e voci registrati all'interno dei luoghi di lavoro aziendali, se non con il preventivo consenso del Responsabile d'ufficio.

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

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

18. Osservanza delle disposizioni in materia di Privacy

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

Gli strumenti tecnologici considerati nel presente Regolamento costituiscono tutti strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa, anche ai sensi e per gli effetti dell'art. 4, comma secondo, della Legge n. 300/1970; conseguentemente, le informazioni raccolte sulla base di quanto indicato nel Regolamento, anche conformemente al successivo punto 13, possono essere utilizzate a tutti i fini connessi al rapporto di lavoro, essendone stata data informazione ai lavoratori sulle modalità di uso degli strumenti stessi, sugli interventi che potranno venir compiuti nel sistema informatico aziendale ovvero nel singolo strumento e sui conseguenti sistemi di controllo che potessero venir eventualmente compiuti (conformemente al successivo punto 14), fermo restando il rispetto della normativa in materia di protezione dei dati personali (GDPR 2016/679).

Viene, infine, precisato che non sono installati o configurati sui sistemi informatici in uso agli utenti apparati hardware o strumenti software aventi come scopo il loro utilizzo come strumenti per il controllo a distanza dell'attività dei lavoratori; peraltro, lì dove l'adozione di tali apparati risultasse necessaria per finalità altre, es. esigenze organizzative e produttive, di sicurezza del lavoro e/o di tutela del patrimonio aziendale, *Istituto* ***Liceo Ariosto-Spallanzani*** provvederà conformemente a quanto disposto dall'art.4, comma primo, della Legge n.300/1970, dandone anche opportuna informazione agli utenti stessi.

19. Accesso ai dati trattati dall'utente

Oltre che per motivi di sicurezza del sistema informatico, compresi i motivi tecnici e/o manutentivi (ad esempio, aggiornamento/sostituzione/implementazione di programmi, manutenzione hardware, etc.), per finalità di controllo e programmazione dei costi aziendali (ad esempio, verifica

costi di connessione ad internet, traffico telefonico, etc.), comunque estranei a qualsiasi finalità di controllo dell'attività lavorativa, è facoltà della Direzione Aziendale, tramite il personale del Servizio ICT o addetti alla manutenzione, accedere direttamente, nel rispetto della normativa sulla privacy, a tutti gli strumenti informatici aziendali e ai documenti ivi contenuti, nonché ai tabulati del traffico telefonico.

20. Sistemi di controlli graduali

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

21. Sanzioni

Un Incaricato che abbia violato le linee guida di sicurezza riportate nel presente documento potrebbe essere sottoposto ad azioni disciplinari, per i possibili riflessi che la sua negligenza potrebbe avere avuto sulla sicurezza relativa alla protezione dei dati personali.