Istituto di Istruzione Secondaria Superiore "R. Gorjux – N. Tridente – C. Vivante"
Polo Tecnico e Professionale Turistico – Grafico – Economico
Direzione e segreteria - SEDE GORJUX: Via Raffaele Bovio, s.n. - 70125 Bari – Tel./Fax: 0805461463 - 0805461506
SEDE TRIDENTE: Via Papa Giovanni XXIII, 59 – Bari - Tel. 0805574381 Fax 0805521551
SEDE ASSOCIATA MOLA: Piazza dei Mille, 20 - 70042 Mola di Bari - Tel. e fax 0804741526
SEDE VIVANTE: Piazza Diaz, 10 – 70121 – Tel. 0805540560 Fax 0805540965
bais03700e@istruzione.it – bais03700e@pec.istruzione.it - www.istitutogorjuxtridentevivante.gov.it – CF 93062330720

Privacy Policy

per l'utilizzo degli strumenti di lavoro adottato dall'Istituto GORJUX - TRIDENTE - VIVANTE

Indice

Premessa

La progressiva diffusione delle nuove tecnologie informatiche e, in particolare, il libero accesso alla rete Internet dai Personal Computer, Tablet, Smartphone e più in generale ogni apparato in gradi di connettersi alla rete, espone **l'Istituto Gorjux-Tridente.Vivante** (nel seguito "**ISTITUTO")** e gli utenti (dipendenti e collaboratori della stessa) a rischi di natura patrimoniale, oltre alle responsabilità penali conseguenti alla violazione di specifiche disposizioni di legge (legislazione sul diritto d'autore e sulla privacy, fra tutte), creando evidenti problemi alla sicurezza ed all'immagine dell'Istituto stesso.

Premesso quindi che l'utilizzo degli strumenti di lavoro, nei quali sono compresi anche i sistemi e le risorse informatiche e telematiche, deve sempre ispirarsi al principio della diligenza e correttezza, propri del rapporto di lavoro, l'Istituto adotta la presente Privacy Policy diretta ad evitare che comportamenti inconsapevoli possano innescare problemi o minacce alla Sicurezza nel trattamento dei dati nonché originare responsabilità in capo all'Istituto ovvero ai singoli lavoratori.

Le prescrizioni di seguito previste si aggiungono ed integrano le specifiche istruzioni fornite a tutti i Soggetti Autorizzati in attuazione del Regolamento 2016/679/UE (nel seguito "GDPR") e del D. lgs. 30 giugno 2003 n. 196 (di seguito "Codice") come modificato dal D. lgs. 101/2018, relativamente alle prescrizioni non in contrasto con il GDPR, nonché integrano le informazioni fornite agli interessati in ordine alle ragioni e alle modalità dei possibili controlli o alle conseguenze di tipo disciplinare in caso di violazione delle stesse. Si tiene conto,purchè non in contrasto con il GDPR, delle principali prescrizioni e le linee guida del Garante privacy in relazione al trattamento di dati personali effettuato dai datori di lavoro, (provvedimento "Linee-guida per il trattamento di dati dei dipendenti" del 23 novembre 2006) ai fini delle verifiche per il corretto utilizzo della posta elettronica e della rete Internet da parte dei dipendenti (provvedimento del 1° marzo 2007) nonché delle previsioni dell'art. 4 l. 300/70, come modificato dal D.lgs. 151/2015 relativamente ai controlli sugli "strumenti di lavoro", e tenendo presente le indicazioni fornite dal WP 29 con la "Opinion 2/2017 on data processing at work".

Dal contesto tracciato dal Garante nelle premesse dei citati provvedimenti emerge che:

- compete ai datori di lavoro assicurare la funzionalità e il corretto impiego di tali mezzi da parte dei lavoratori, definendone le modalità d'uso nell'organizzazione dell'attività lavorativa, tenendo conto della disciplina in tema di diritti e relazioni sindacali;
- spetta sempre ai datori di lavoro adottare idonee misure di sicurezza per assicurare la disponibilità e l'integrità di sistemi informativi e dei dati, anche per prevenire utilizzi indebiti che possono essere fonte di responsabilità;
- è necessario tutelare i lavoratori interessati anche perché l'utilizzazione dei predetti mezzi, già ampiamente diffusi nel contesto lavorativo, è destinata ad un rapido incremento in numerose attività svolte anche fuori della sede lavorativa;
- l'utilizzo di Internet da parte dei lavoratori può infatti formare oggetto di analisi, profilazione e integrale ricostruzione mediante elaborazione di file di log, della navigazione web ottenuti, ad esempio, da un proxy server o da un altro strumento di registrazione delle informazioni. I servizi di posta elettronica sono parimenti suscettibili (anche attraverso la tenuta dei file di log di traffico e-mail e l'archiviazione di messaggi) di controlli che possono giungere fino alla conoscenza da parte del datore di lavoro (titolare del trattamento) del contenuto della corrispondenza;

- le informazioni così trattate contengono dati personali anche sensibili riguardanti lavoratori o terzi, identificati o identificabili.

Alla luce delle premesse sopra riportate ed avendo in considerazione che l'Istituto nell'ottica di uno svolgimento proficuo e più agevole della propria attività, ha da tempo deciso di mettere a disposizione dei propri collaboratori che ne necessitassero per il tipo di funzioni svolte, telefoni e mezzi di comunicazione efficienti (computer desk-top e/o portatili, telefoni cellulari, etc.), sono state inserite in questo documento le opportune indicazioni ed istruzioni relative alle modalità ed ai doveri che ciascun lavoratore deve osservare nell'utilizzo di tale strumentazione.

1. Entrata in vigore del regolamento e pubblicità

1.1 Con l'entrata in vigore del presente Privacy Policy tutte le disposizioni in precedenza adottate in materia, in qualsiasi forma comunicate, devono intendersi abrogate e sostituite dalle presenti.

1.2 Copia di questo documento viene pubblicato sul sito istituzionale dell'Istituto, ed allegato alla comunicazione che ne ufficializza l'adozione nelle forme e con le modalità in uso presso l'Istituto.

2. Campo di applicazione

2.1 La Privacy Policy si applica a tutti i lavoratori, ossia ai dipendenti, senza distinzione di ruolo e/o livello, nonché a tutti i collaboratori dell'Istituto a prescindere dal rapporto contrattuale con la stessa intrattenuto.

2.2 Ai fini delle disposizioni dettate per l'utilizzo delle risorse informatiche e telematiche, per "utente" deve intendersi ogni lavoratore in possesso di specifiche credenziali di autenticazione. Tale figura sarà anche indicata quale "Soggetto Autorizzato al trattamento" nell'accezione propria dell'art. 29 del GDPR.

3. Utilizzo del Personal Computer

3.1 **Il Personal Computer affidato all'utente 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. Il personal computer (PC) deve essere custodito con cura evitando ogni possibile forma di danneggiamento.

3.2 Il personal computer dato in affidamento all'utente permette l'accesso alla rete solo attraverso specifiche **credenziali di autenticazione** come meglio descritto al successivo punto 4 del presente documento.

3.3 Il personale nominato Soggetto Autorizzato, per l'espletamento delle sue funzioni e per garantire la sicurezza del sistema informatico, ha la facoltà, in qualunque momento, di accedere ai dati trattati da ciascuno, ivi compresi gli archivi di posta elettronica, come più specificatamente precisato al successivo punto 13.1 del presente documento. La stessa facoltà, sempre ai fini della sicurezza del sistema e per garantire la normale operatività dell'Istituto, si applica anche in caso di assenza prolungata od impedimento dell'utente. Analoghe verifiche possono essere effettuate sui siti internet acceduti dagli utenti abilitati alla navigazione esterna. L'accesso, comunque, verrà effettuato con modalità tali da evitare qualsiasi forma di controllo a distanza. In ogni caso, l'Istituto

garantisce la non effettuazione di alcun trattamento mediante sistemi *hardware* e *software* specificatamente preordinati al controllo a distanza, quali, a titolo esemplificativo:

- lettura e 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*;
- riproduzione ed eventuale memorizzazione sistematica delle pagine *web* visualizzate dal lavoratore;
- la lettura e la registrazione dei caratteri inseriti tramite la tastiera o analogo dispositivo;
- l'analisi occulta di computer portatili affidati in uso.

3.4 Non è consentito l'uso di programmi diversi da quelli ufficialmente installati né viene consentito agli utenti di installare autonomamente programmi provenienti dall'esterno, sussistendo infatti il grave pericolo di introdurre Virus informatici e/o di alterare la funzionalità delle applicazioni software esistenti. L'inosservanza della presente disposizione espone lo stesso Istituto a gravi responsabilità civili; si evidenzia inoltre che le violazioni della normativa a tutela dei diritti d'autore sul software che impone la presenza nel sistema di software regolarmente licenziato, o comunque libero e quindi non protetto dal diritto d'autore, vengono sanzionate anche penalmente.

3.6 Salvo preventiva espressa autorizzazione del Delegato Interno al trattamento, non è consentito all'utente modificare le caratteristiche impostate sul proprio PC né procedere ad installare dispositivi di memorizzazione, comunicazione o altro (come ad esempio masterizzatori, modem, etc.).

3.7 Ogni utente deve prestare la massima attenzione ai supporti di origine esterna, avvertendo immediatamente il Delegato Interno al trattamento nel caso in cui siano rilevati virus ed adottando quanto previsto dal successivo punto 10 del presente Regolamento relativo alle procedure di protezione antivirus.

3.8 Il Personal Computer deve essere spento prima di lasciare gli uffici o in caso di assenze prolungate dall'ufficio o in caso di suo inutilizzo. In ogni caso, 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. Al fine di evitare tali evenienze si dovrà "bloccare" l'utilizzo del PC prima di allontanarsi o impostare la modalità "screen saver" che prevede la richiesta della password per riattivarne l'uso**.**

4. Gestione ed assegnazione delle credenziali di autenticazione

4.1 Le credenziali di autenticazione per l'accesso alla rete vengono assegnate dal Delegato Interno al trattamento, previa formale richiesta.

4.2 Le credenziali di autenticazione consistono in un codice per l'identificazione dell'utente (user id), associato ad una parola chiave (password) riservata che dovrà venir custodita dal Soggetto Autorizzato con la massima diligenza e non divulgata. Non è consentita l'attivazione della password di accensione (bios), senza preventiva autorizzazione da parte del Delegato Interno al trattamento.

4.3 La parola chiave, formata da lettere (maiuscole o minuscole) e/o numeri, anche in combinazione fra loro, deve essere composta da almeno otto caratteri e non deve

contenere riferimenti agevolmente riconducibili al Soggetto Autorizzato. Per costruire la password utilizzare:

- lettere, numeri e almeno un carattere tra . ; $! @ - > <
- Non utilizzare date di nascita, nomi o cognomi propri o di parenti
- Non sceglierla uguale alla matricola o alla userid
- Custodirla sempre in un luogo sicuro e non accessibile a terzi
- Non divulgarla a terzi e non condividerla con altri utenti

4.4 È necessario procedere alla modifica della parola chiave a cura dell'utente, ove ciò non avvenga grazie a processi automatici del sistema informativo, al primo utilizzo e, successivamente, almeno ogni sei mesi (Ogni tre mesi nel caso invece di trattamento di dati sensibili attraverso l'ausilio di strumenti elettronici).

4.5 Qualora la parola chiave dovesse venir sostituita, per decorso del termine sopra previsto e/o in quanto abbia perduto la propria riservatezza, si procederà in tal senso d'intesa con il Delegato Interno al trattamento.

5. Utilizzo della rete interna

5.1 Per l'accesso alla rete dell'Istituto ciascun utente deve essere in possesso della specifica credenziale di autenticazione.

5.2 È assolutamente proibito entrare nella rete e nei programmi con un codice d'identificazione utente diverso da quello assegnato. Le parole chiave d'ingresso alla rete ed ai programmi sono segrete e vanno comunicate e gestite secondo le istruzioni impartite.

5.3 Le cartelle utenti presenti nei server dell'Istituto sono aree di condivisione di informazioni strettamente professionali e non possono in alcun modo essere utilizzate per scopi diversi. Pertanto, qualunque file che non sia legato all'attività lavorativa non può essere dislocato, nemmeno per brevi periodi, in queste unità. Su queste unità vengono svolte regolari attività di controllo, amministrazione e back up da parte del Delegato Interno al trattamento. Si ricorda che tutti i dischi o altre unità di memorizzazione locali (es. disco C: interno PC) non sono soggette a salvataggio da parte del personale nominato Soggetto Autorizzato. La responsabilità del salvataggio dei dati ivi contenuti è pertanto a carico del singolo utente.

5.4 Il Delegato Interno al trattamento può in qualunque momento procedere alla rimozione di ogni file o applicazione che riterrà essere pericolosi per la Sicurezza sia sui PC dei Soggetti Autorizzati sia sulle unità di rete.

5.5 Risulta opportuno che, con regolare periodicità (almeno ogni tre mesi), ciascun utente provveda alla pulizia degli archivi del proprio PC, con cancellazione dei file obsoleti o inutili. Particolare attenzione deve essere prestata alla duplicazione dei dati, essendo infatti necessario evitare un'archiviazione ridondante.

6. Utilizzo e conservazione dei supporti rimovibili

6.1 Tutti i supporti magnetici rimovibili (CD e DVD riscrivibili, supporti USB, hard-disk removibili, ecc.), contenenti dati rilevanti, devono essere trattati con particolare cautela onde evitare che il loro contenuto possa essere trafugato o alterato e/o distrutto o, successivamente alla cancellazione, recuperato.

6.2 Al fine di assicurare la distruzione e/o inutilizzabilità di supporti magnetici rimovibili contenenti dati sensibili, ciascun utente dovrà contattare il Delegato Interno al trattamento e seguire le istruzioni da questo impartite.

6.3 In ogni caso, i supporti magnetici contenenti dati **particolari/sensibili**, secondo la definizione dell'art. 4 del GDPR, devono essere adeguatamente custoditi dagli utenti e risposti in armadi chiusi ad accesso controllato.

6.4 È vietato l'utilizzo di supporti rimovibili personali.

6.5 L'utente è responsabile della custodia dei supporti e dei dati personali in essi contenuti.

7. Utilizzo di PC portatili

7.1 L'utente è responsabile del PC portatile assegnatogli dal Delegato Interno al trattamento e deve custodirlo con diligenza sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro.

7.2 Ai PC portatili si applicano le regole di utilizzo previste per i PC desktop.

7.3 I PC portatili utilizzati all'esterno, in caso di allontanamento, devono essere custoditi con diligenza, adottando tutti i provvedimenti che le circostanze rendono necessari per evitare danni o sottrazioni.

8. Uso della posta elettronica

8.1 **La casella di posta elettronica assegnata all'utente è uno strumento di lavoro.** Le persone assegnatarie delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse.

8.2 È fatto divieto di utilizzare le caselle di posta elettronica istituzionali per motivi diversi da quelli strettamente legati all'attività lavorativa. In questo senso, a titolo puramente esemplificativo, l'utente non potrà utilizzare la posta elettronica per:

- l'invio e/o il ricevimento di allegati contenenti filmati o brani musicali (es.mp3) non legati all'attività lavorativa;
- l'invio e/o il ricevimento di messaggi personali o per la partecipazione a dibattiti, aste on line, concorsi, forum o mailing-list;
- la partecipazione a catene telematiche. Se si dovessero peraltro ricevere messaggi di tale tipo, si deve comunicarlo immediatamente al Delegato Interno al trattamento. Non si dovrà in alcun caso procedere all'apertura degli allegati a tali messaggi.

8.3 La casella di posta deve essere mantenuta in ordine, cancellando documenti inutili.

8.4 Ogni comunicazione inviata o ricevuta che abbia contenuti rilevanti o contenga impegni contrattuali o precontrattuali per l'Istituto ovvero contenga documenti da considerarsi riservati, deve essere preventivamente visionata od autorizzata dal Delegato Interno al trattamento.

8.5 È possibile utilizzare la ricevuta di ritorno per avere la conferma dell'avvenuta lettura del messaggio da parte del destinatario. Si evidenzia però che le comunicazioni ufficiali, da inviarsi mediante gli strumenti tradizionali, possono richiedere l'autorizzazione e la firma dei Responsabili di ufficio, a seconda del loro contenuto e dei destinatari delle stesse.

8.6 È obbligatorio controllare i file attachment di posta elettronica prima del loro utilizzo (non eseguire download di file eseguibili o documenti da siti Web o Ftp non conosciuti).

8.7 Al fine di ribadire agli interlocutori la natura esclusivamente istituzionale della casella di posta elettronica, i messaggi devono contenere un avvertimento standardizzato nel quale sia dichiarata la natura non personale dei messaggi stessi precisando che, pertanto, personale dipendente dell'Istituto debitamente nominato Soggetto Autorizzato potrà accedere al contenuto del messaggio inviato alla stessa casella secondo le regole fissate nel presente documento. Si riportano di seguito i testi da utilizzare:

Le informazioni contenute nella presente e-mail potrebbero essere confidenziali e sono dirette unicamente ai destinatari sopra indicati. In caso di ricezione da parte di persona diversa è vietato qualunque tipo di distribuzione o copia. Chi riceva questo messaggio per errore è pregato di inoltrarlo al mittente e di distruggere questa e-mail.

8.8 Come anticipato al precedente punto 3.3 del presente documento, il personale nominato Soggetto Autorizzato potrà accedere ai dati contenuti nelle caselle di posta elettronica di lavoro per le sole finalità ivi indicate.

9. Navigazione in Internet

9.1. **Il PC assegnato al singolo utente ed abilitato alla navigazione in Internet costituisce uno strumento istituzionale 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.

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

- l'upload o il download di software 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 Delegato Interno al trattamento);
- 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 dall'Istituto (o eventualmente dal Delegato Interno al trattamento) 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'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 Delegato Interno al trattamento;
- l'accesso, tramite Internet, a caselle webmail di posta elettronica personale, salvo specifica autorizzazione.

9.3 Al fine di evitare la navigazione in siti non pertinenti all'attività lavorativa, l'Istituto può prevedere l'adozione di uno specifico sistema di blocco o filtro automatico che prevengano determinate operazioni quali l'upload o l'accesso a specificati siti inseriti in una black list.

9.4 In conformità al punto 3.3, il personale nominato Soggetto Autorizzato potrà procedere a controlli sulla navigazione finalizzati esclusivamente a garantire l'operatività e la sicurezza del sistema, nonché il necessario svolgimento delle attività lavorative, es. mediante un sistema di controllo dei contenuti (Proxy server) o mediante "file di log" della navigazione svolta. Il controllo sui file di log non è continuativo ed i file stessi vengono conservati non oltre 6 mesi.

10. Protezione antivirus

10.1 Il sistema informatico dell'Istituto è protetto da software antivirus aggiornato periodicamente. Ogni utente deve comunque tenere comportamenti tali da ridurre il rischio di attacco al sistema informatico istituzionale mediante virus o mediante ogni altro software aggressivo.

10.2 Nel caso il software antivirus rilevi la presenza di un virus, l'utente dovrà immediatamente sospendere ogni elaborazione in corso senza spegnere il computer nonché segnalare prontamente l'accaduto al Delegato Interno al trattamento.

10.3 Ogni dispositivo magnetico di provenienza esterna all'Istituto dovrà essere verificato mediante il programma antivirus prima del suo utilizzo e, nel caso venga rilevato un virus, dovrà essere prontamente consegnato al Delegato Interno al trattamento.

11. Utilizzo dei telefoni e fotocopiatrici dell'Istituto.

11.1 L'eventuale telefono affidato al lavoratore è uno strumento di lavoro. Ne viene concesso l'uso esclusivamente per lo svolgimento dell'attività lavorativa, non essendo quindi consentite comunicazioni a carattere personale o comunque non strettamente inerenti all'attività lavorativa stessa. La ricezione o l'effettuazione di telefonate personali è consentita sempre che vengano rispettati i criteri di ragionevolezza ovvero nel caso di necessità ed urgenza.

11.2 Qualora venisse assegnato un cellulare (o smartphone, tablet, etc.) istituzionale all'utente, quest'ultimo sarà responsabile del suo utilizzo e della sua custodia. Al cellulare istituzionale si applicano le medesime regole sopra previste per l'utilizzo del telefono istituzionale: in particolare è vietato l'utilizzo del telefono cellulare messo a disposizione per inviare o ricevere SMS di natura personale o comunque non pertinenti rispetto allo svolgimento dell'attività lavorativa. L'eventuale uso promiscuo (anche per fini personali) del telefono cellulare istituzionale è possibile soltanto in presenza di preventiva autorizzazione scritta e in conformità delle istruzioni al riguardo impartite dall'Istituto.

11.3 È vietato l'utilizzo delle fotocopiatrici per fini personali, salvo preventiva ed esplicita autorizzazione da parte del Delegato Interno al trattamento.

12. Osservanza delle disposizioni in materia di Privacy

12.1 È obbligatorio attenersi alle disposizioni in materia di protezione dei dati personali previste dal GDPR, e dal Codice, rispettando le misure di sicurezza adottate dall'Istituto, nonché le istruzioni fornite con la designazione a "Soggetto Autorizzato al trattamento dei dati", come previsto dall'art. 29 del GDPR, applicando puntualmente le disposizioni ivi contenute nonché ogni ulteriore indicazione comunicata, anche per le vie brevi, dal Delegato Interno al trattamento.

12.2 I "Soggetti Autorizzati" che sono addetti alle attività di amministrazione e gestione dei Sistemi, Data Base e della Infrastruttura di connessione dovranno rispettare le specifiche istruzioni loro fornite al fine di rispettare i principi di necessità e di legittimità e correttezza nella effettuazione delle loro attività. I nominativi di coloro che hanno competenza sui sistemi che trattano dati personali dei dipendenti dell'Istituto potranno essere comunicati nelle modalità e con le forme previste dalla normativa applicabile.

13. Accesso ai dati trattati dall'utente

13.1 Oltre che per motivi di sicurezza del sistema informatico, anche per motivi tecnici e/o manutentivi (ad esempio, aggiornamento/sostituzione/implementazione di programmi, manutenzione hardware, etc.) comunque estranei a qualsiasi finalità di controllo dell'attività lavorativa, è facoltà dell'Istituto, accedere direttamente, nel rispetto della normativa sulla privacy, a tutti gli strumenti informatici istituzionali e ai documenti ivi contenuti, nonché ai tabulati del traffico telefonico.

14. Gestione Archivi cartacei

14.1 Quando si tratta di applicare e adottare il GDPR, per i documenti cartacei come per qualsiasi informazione personale detenuta, i soggetti autorizzati dell'Istituto devono esaminare le modalità di archiviazione delle informazioni e agire secondo le seguenti regole.

14.2 Stampare semplicemente un documento e dimenticarsi di averlo fatto può costituire un rischio per la sicurezza e bisogna considerare che dei soggetti non autorizzati potrebbero accidentalmente prendere quel documento stampato.
Ogni volta che si invia un documento da stampare tramite una stampante wireless o di rete, si corre il rischio di violazioni della sicurezza.

14.3. I documenti cartacei da conservare devono essere gestiti in modo da poter essere rintracciati e individuati facilmente. I documenti cartacei contenenti dati particolari sensibili o giudiziari devono essere conservati in armadietti chiusi a chiave il cui accesso è limitato soltanto alle persone autorizzate a quel trattamento all'interno dell'Istituto.

14.4. Lo smaltimento sicuro della carta deve essere una priorità, in particolare ora che l'UE ha aumentato le sue richieste in materia di protezione dei dati. I documenti cartacei non più necessari devono essere smaltiti in modo conforme. Bisogna utilizzare la macchina distruggidocumenti o in mancanza agire manualmente spezzettando i fogli in piccole parti in modo da non essere più ricomponibili.

14.5 I documenti cartacei contenenti dati personali devono essere custoditi in modo da non essere accessibili a persone non autorizzate al trattamento (es. armadi o cassetti chiusi a chiave).

I documenti cartacei che vengono prelevati dagli archivi per l'attività quotidiana devono esservi riposti nel periodo di intervallo meridiano e a fine giornata e non devono rimanere incustoditi su scrivanie o tavoli di lavoro.

14.6 I documenti cartacei contenenti dati particolari sensibili o giudiziari devono essere controllati e custoditi dai soggetti autorizzati in modo che non vi possano accedere persone prive di autorizzazione. La loro consultazione deve avvenire per il tempo strettamente necessario alla necessità di utilizzo e, subito dopo, i documenti devono essere nuovamente archiviati.

14.7 La presenza di ospiti o di personale non autorizzato non è consentita in luoghi in cui siano presenti documenti cartacei in vista.

14.8 Evitare assolutamente di prendere appunti su fogli di carta accumulati per il riciclo senza badare a ciò che è stampato sul retro: tipicamente si tratta di vecchi documenti stampati che possono contenere dati personali e particolari sensibili o giudiziari.

15. Sistemi di controlli graduali

15.1 In caso di anomalie e su mandato dell'Istituto, il personale nominato Soggetto Autorizzato del trattamento o gli addetti alla manutenzione, 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 istituzionali e si inviteranno gli utenti ad attenersi scrupolosamente ai compiti assegnati e alle istruzioni impartite. Controlli su base individuale potranno essere computi solo in caso di successive ulteriori anomalie.

15.2 In alcun caso verranno compiuti controlli prolungati, costanti o indiscriminati.

16. Sanzioni

16.1 È fatto obbligo a tutti i lavoratori di osservare le disposizioni portate a conoscenza con il presente documento. Il mancato rispetto o la violazione delle regole sopra ricordate possono di per sé considerarsi contrari ai doveri di diligenza e fedeltà previsti dagli artt. 2104 e 2105 del Codice civile e sono perseguibili nei confronti del personale dipendente con provvedimenti disciplinari e risarcitori previsti dal Contratto di lavoro sottoscritto ovvero dal vigente CCNL, nonché con tutte le azioni civili e penali consentite.

17. Aggiornamento e revisione

17.1 Tutti gli utenti possono proporre, quando ritenuto necessario, integrazioni motivate al presente documento. Le proposte verranno esaminate dall'Istituto.

17.2 Il presente documento è soggetto a revisione con frequenza periodica anche in funzione dell'introduzione di nuovi strumenti di lavoro e/o informatici, dell'evoluzione tecnologica o di cambiamenti normativi.