ISTITUTO ISTRUZIONE SUPERIORE		
porro@alberti-porro.edu.it porro@pec.it	**“Ignazio Porro”** Sede: Viale Kennedy, 30 – PINEROLO (TO) ☎ 0121/39.13.11 - 🖷 0121/39.13.99 **C.F. 94540190017 www.alberti-porro.edu.it**	tois01400d@istruzione.it tois01400d@pec.istruzione.it

ISTRUZIONI OPERATIVE ALLE PERSONE AUTORIZZATE AL TRATTAMENTO

ai sensi del Regolamento UE n. 2016/679 - relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e del Principio di Accountability

Data	Revisione	Descrizione
11/11/2019	00	Prima emissione

GESTIONE DEGLI STRUMENTI ELETTRONICI

Ciascun autorizzato è responsabile del corretto utilizzo e della custodia degli strumenti elettronici in dotazione (a titolo esemplificativo personal computer, periferiche, lettori di smart card) ed è tenuto a custodirli con diligenza sia nel corso degli spostamenti che durante l'utilizzo nel luogo di lavoro. È necessario che egli adotti misure di sicurezza adeguate alla tutela della riservatezza, onde evitare l'accesso ai dati da parte di soggetti estranei all'Istituto o non specificamente autorizzati.

Per una corretta gestione della sessione di lavoro sul pc:

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

Per l'utilizzo dei PC portatili valgono le seguenti ulteriori raccomandazioni:

- prima della riconsegna, l'autorizzato deve rimuovere eventuali file ivi elaborati;
- quando il PC portatile è nei locali dell'Azienda, deve evitare di lasciarlo incustodito; in caso di brevi assenze è necessario che egli si assicuri di avere attive misure di protezione adeguate al fine di evitare l'accesso al PC da parte di soggetti non autorizzati, e ove possibile è consigliato chiudere a chiave la porta dell'ufficio;
- quando il PC portatile è all'esterno dell'Azienda, non deve mai lasciarlo incustodito;
- in caso di furto di un portatile deve avvertire tempestivamente il responsabile del Servizio Informatico, onde prevenire possibili intrusioni ai sistemi aziendali;
- deve eseguire periodicamente salvataggi dei dati e non tenere tali backup insieme al PC portatile;
- nell'eventualità in cui venisse a mancare la fornitura di energia elettrica, si consiglia all'autorizzato, trascorsi cinque minuti dall'interruzione dell'erogazione, di provvedere alla chiusura di tutti gli applicativi utilizzati al fine di salvaguardare l'integrità dei dati elaborati e procedere allo spegnimento del PC.

GESTIONE PROTEZIONE DAI VIRUS INFORMATICI

Per prevenire eventuali danneggiamenti al software causati dalla presenza o dall'azione di programmi virus informatici, gli elaboratori aziendali sono dotati di un software antivirus. L'antivirus aziendale non deve mai essere disattivato o sostituito con altro antivirus non ufficialmente fornito.

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

Si raccomanda di non scaricare e né tantomeno aprire file provenienti via e-mail da mittenti sconosciuti. Tali file, potrebbero essere portatori di virus e compromettere la funzionalità del PC, l'integrità dei dati in esso contenuti e soprattutto l'integrità dei sistemi collegati al PC stesso.

GESTIONE USERNAME E PASSWORD

A ciascun utilizzatore del sistema informativo è assegnato un identificatore d'accesso (denominato username) per poter accedere all'elaboratore elettronico ed alle risorse di rete (gestionali, registro elettronico, documenti, applicazioni, email, ecc.) o, tramite connessione internet, ad altri sistemi esterni (home banking, ecc..).

Alla username è abbinata una chiave di accesso (password) necessaria per poter utilizzare la username stessa: la coppia di informazioni composta da login-id e password garantisce l'identità e l'univocità dell'utilizzatore. Per tale motivo, e sotto la responsabilità dell'utente, la password deve essere mantenuta segreta e non comunicata, o ancor peggio condivisa con altri. Allo stesso modo la password non deve mai essere trascritta su supporto cartaceo, evitando dunque di apporre post-it riportanti la password di accesso in prossimità della propria postazione o comunque all'interno della struttura. Qualora si ritenga che la segretezza della propria password sia stata violata, si deve provvedere immediatamente cambiandola.

Le credenziali di accesso alla "postazione di lavoro" sono fornite dal tecnico informatico all'autorizzato al momento dell'assunzione. Alla prima assegnazione, l'utente – non appena effettuata l'autenticazione – provvederà a modificare autonomamente la propria password. Ogni sei mesi ciascun autorizzato dovrà provvede a sostituire la propria password.

La password dovrà rispondere ai seguenti requisiti minimi di sicurezza:

- deve essere costituita da una sequenza di minimo otto caratteri alfanumerici, oppure, nel caso che lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito;
- non deve essere facilmente individuabile;
- non deve contenere riferimenti riconducibili all'autorizzato (es.: cognome, nome, codice di accesso, etc...);
- deve contenere almeno un carattere alfabetico ed uno numerico;
- non deve contenere la username;
- non deve essere simile alla password precedente.

GESTIONE DELLA POSTA ELETTRONICA AZIENDALE

Il servizio di posta elettronica viene fornito per permettere la comunicazione con soggetti terzi interni ed esterni per le finalità dell'Istituto e in stretta connessione con l'effettiva attività e mansioni dell'autorizzato che utilizza tale funzionalità.

Al fine di non compromettere la sicurezza della struttura e di prevenire conseguenze legali a carico della stessa, è necessario adottare le seguenti norme comportamentali:

- se si ricevono mail da destinatari sconosciuti contenenti file di qualsiasi tipo, procedere alla loro immediata eliminazione;
- la casella di posta elettronica assegnata deve essere mantenuta in ordine;
- è fatto divieto di utilizzare le caselle di posta elettronica per l'invio di messaggi personali o per la partecipazione a dibattiti, forum o mail list, salvo diversa ed esplicita autorizzazione;
- nell'ipotesi in cui la email debba essere utilizzata per la trasmissione di dati particolari si raccomanda di prestare attenzione a che:
    - l'indirizzo del destinatario sia stato correttamente digitato,
    - l'oggetto del messaggio non contenga direttamente il riferimento a stati, fatti o qualità idonei a rivelare dati di natura sensibile;
    - nel corpo del messaggio sia presente un'intestazione standardizzata in cui si avverta della confidenzialità/riservatezza del messaggio.
- nel caso in cui l'autorizzato cessi il rapporto di lavoro presso l'Istituto, resta inteso che la documentazione presente nel profilo dell'utente verrà considerata presuntivamente dell'istituto, quale corrispondenza e documentazione lavorativa e non personale.

UTILIZZO DELLA RETE

Le unità di rete sono aree di condivisione di informazioni strettamente professionali e non possono in alcun modo essere utilizzate per scopi diversi. Pertanto non si deve salvare in queste unità, nemmeno per brevi periodi, alcun file che non sia legato all'attività lavorativa.

Qualora la cartella di salvataggio delle scansioni effettuate sia in rete, e quindi visibile a tutti gli operatori, sarà necessario che ciascuno di essi abbia cura di cancellare immediatamente dalla cartella condivisa i file scansionati contenenti dati personali e di procedere al salvataggio degli stessi in una cartella locale non visibile ad altri utenti.

UTILIZZO DI COLLEGAMENTI INTERNET

Sono vietati i collegamenti ad Internet per usi non strettamente connessi al lavoro da svolgere e devono essere evitate tutte le attività non strettamente necessarie (come ad esempio l'utilizzo di siti Internet per ascoltare radio, download di film, canzoni, ecc.). Non è ammesso l'utilizzo di collegamenti per servizi o scopi personali. (quali servizi di Borsa, prenotazione viaggi, ecc..).

INSTALLAZIONE DI HARDWARE E SOFTWARE

L'installazione di hardware e software, nonché la modifica dei parametri di configurazione, possono essere eseguite esclusivamente dal tecnico informatico competente.

Pertanto si raccomanda agli utenti dei PC di rispettare i seguenti divieti:

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

GESTIONE DEI SUPPORTI RIMOVIBILI

I supporti rimovibili, come ad esempio dischi magnetici esterni, penne USB o CD riscrivibili, quando contengono dati personali devono essere custoditi in luogo protetto e non accessibile (cassaforte, armadio chiuso a chiave, ecc..). Quando non sono più utilizzati devono essere distrutti o resi inutilizzabili, ovvero possono essere riutilizzati da altri soggetti non autorizzati al trattamento degli stessi dati, soltanto dopo essere stati formattati.

Il trasferimento di file contenenti dati personali, dati particolari su supporti rimovibili è da eseguire unicamente in via transitoria, ponendo la massima attenzione alla destinazione di trasferimento e cancellando i file appena possibile.

Gli autorizzati al trattamento dei dati personali hanno la responsabilità di:

- segnalare la necessità di un'eventuale riparazione degli hard disk;
- segnalare la necessità di un eventuale riutilizzo degli hard disk.

LIMITAZIONI O ESCLUSIONE DI ATTIVITÀ NELL'USO DELLE RISORSE INFORMATICHE

Per effettuare i trattamenti previsti dalla mansione, ad ogni utente viene concesso l'utilizzo di alcune risorse informatiche (sistemi hardware, programmi e applicazioni software, apparati di rete, risorse di stampa), le quali costituiscono strumenti di esecuzione delle normali prestazioni di lavoro.
Il loro uso deve sempre essere improntato al principio di comune buon senso e di civiltà. Pertanto, al fine di garantire la funzionalità, la sicurezza ed il corretto impiego degli strumenti elettronici e, al tempo stesso, garantire un elevato livello di sicurezza dei trattamenti e assicurare la protezione della riservatezza di dipendenti e collaboratori, alcuni comportamenti (indicati di seguito) sono vietati.

Comportamenti vietati rispetto all'utilizzo del Personal Computer

È fatto espresso divieto di:

- accedere e utilizzare le risorse ed i servizi per motivi non lavorativi o non di servizio;
- usare le risorse o i servizi in violazione di normative comunitarie, leggi, regolamenti, provvedimenti, prescrizioni, o commettere attività illecite o discriminanti;
- modificare le configurazioni impostate;
- installare e utilizzare prodotti software che non siano stati autorizzati;
- installare e utilizzare software che consentano di intercettare il traffico o violare le password;
- usare le risorse o i servizi per scopi commerciali, promozionali, pubblicitari;
- utilizzare eccessivo spazio disco o assorbire capacità di banda nei sistemi di telecomunicazione, attraverso la generazione o l'invio di mail non strettamente correlate all'attività lavorativa, o in generale, attraverso il trasferimento di file o messaggi di dimensioni eccessive;
- inviare o depositare sui computer materiale di natura illegale o discriminante;
- mascherare la propria identità all'interno dei sistemi informatici;
- utilizzare le credenziali di autenticazione di altri utenti, per qualsivoglia ragione;
- tentare di violare password, sistemi di protezione, restrizioni imposte dal sistema;
- riprodurre o distribuire materiale in formato digitale senza autorizzazione;
- copiare o modificare files, redatti da altri utenti, senza autorizzazione;
- alterare i dati, introdurre o diffondere virus, trojan, backdoor, dataminer o altri codici malefici;
- interferire con il corretto funzionamento o danneggiare le attrezzature di rete;
- intercettare o alterare qualunque tipo di dato o di comunicazione digitale.

Comportamenti vietati rispetto all'utilizzo di internet

È fatto espresso divieto di:

- navigare su siti non correlati con la prestazione lavorativa;
- effettuare download di programmi e files estranei al lavoro;
- partecipare a forum, accedere e utilizzare chat line, partecipare ad aste on-line;
- scaricare, copiare, conservare, diffondere file a contenuto offensivo, discriminatorio, pedofilo, o di altro contenuto illecito penalmente o civilmente;
- accedere a siti di gioco, pornografici o con finalità ludiche;
- attivare strumenti di videochiamata (es.: skype).

Comportamenti vietati rispetto all'utilizzo della posta elettronica

È fatto espresso divieto di:

- utilizzare la posta elettronica per ragioni non attinenti ai compiti affidati;
- inviare, stampare, conservare messaggi offensivi o discriminatori;
- comunicare indirizzi di posta riconducibili al Titolare per partecipare a dibattiti, forum o mailing list di contenuto non pertinente con lo svolgimento delle mansioni affidate;
- creare cartelle segrete o nascoste per la conservazione dei messaggi.

GESTIONE DEGLI STRUMENTI NON ELETTRONICI

Per quanto riguarda l'archiviazione dei documenti cartacei, è necessario che essi siano tenuti in archivi adeguatamente protetti, per evitarne la lettura e/o il prelievo non autorizzato e per garantire, quindi, la riservatezza e l'integrità dei dati in essi contenuti.

Al termine della giornata lavorativa, gli archivi dovranno essere chiusi a chiave e le chiavi dovranno essere riposte in luogo sicuro e non lasciate nelle serrature stesse.

La consultazione dei documenti contenenti dati personali e/o particolari, deve avvenire esclusivamente da parte degli Autorizzati al trattamento, solo quando operativamente necessario e, quando possibile, in loco.

Tutti i documenti cartacei decorsi i termini di conservazione previsti dalla legge e/o dal Titolare devono essere distrutti attraverso opportuni strumenti che rendano impossibile la ricostruzione del documento.

Occorre evitare di gettare la documentazione nel cestino della carta straccia senza aver previamente provveduto a rendere inintelligibile il contenuto. Qualora sia necessario distruggere i documenti contenenti dati personali, questi devono essere distrutti utilizzando gli appositi apparecchi "distruggi documenti" o, in assenza, devono essere sminuzzati in modo da non essere più ricomponibili.

Coloro che procedono alla duplicazione di documentazione (con stampanti, fotocopiatrici o altre periferiche) ovvero utilizzino strumenti per la riproduzione cartacea di documenti digitali sono tenuti alla distruzione del relativo supporto qualora si verifichino errori o la riproduzione non sia corretta. È inoltre opportuno evitare di riutilizzare fogli contenenti dati personali.

Gli autorizzati al trattamento qualora trattino documenti cartacei contenenti dati personali e/o sensibili e/o giudiziari sono tenuti ad attenersi alle seguenti prescrizioni:

- è severamente vietato l'accesso a documenti contenenti dati personali per esigenze non strettamente lavorative, connesse ai trattamenti dichiarati, autorizzati e tutelati dal Titolare;
- la documentazione contenente dati personali che, per ragioni di praticità operativa, risiede sulle scrivanie degli autorizzati deve essere rimossa al termine dell'orario di lavoro;
- l'accesso ai supporti deve essere limitato al tempo necessario a svolgere i Trattamenti previsti e gli stessi devono essere archiviati in ambiente ad accesso controllato;
- è vietato lasciare incustoditi in ambienti non controllati documenti contenenti dati personali (ad es. a seguito di stampa su stampante di rete);
- la distruzione dei documenti contenenti dati personali deve essere operata, ove possibile, direttamente dal personale autorizzato. È inoltre severamente vietato utilizzare documenti contenenti dati personali, dati particolari come carta da riciclo o da appunti;
- ove non siano disponibili strumenti per la distruzione dei documenti (trita documenti), o il volume di questi sia tale da imporre il ricorso al servizio di macero, il personale autorizzato che avvia al macero la documentazione è tenuto a confezionare tale documentazione in modo che il pacco risulti anonimo e solido;
- gli atti e i documenti contenenti dati personali, dati particolari (ex dati sensibili) o giudiziari affidati agli autorizzati per lo svolgimento dei relativi compiti devono essere controllati e custoditi dagli autorizzati stessi fino alla restituzione, in modo tale che ad essi non possano accedervi persone prive di autorizzazione, e devono essere restituiti al termine delle operazioni affidate;
- l'accesso agli archivi contenenti dati particolari deve essere controllato. Le persone ammesse, a qualunque titolo, dopo l'orario di chiusura, sono identificate e registrate. Quando gli archivi non sono dotati di strumenti elettronici per il controllo degli accessi o di autorizzati alla vigilanza, le persone che vi accedono devono essere preventivamente autorizzate;
- i documenti (o copia degli stessi) non possono, senza specifica autorizzazione, essere portati fuori dai luoghi di lavoro, salvo i casi di comunicazione dei dati a terzi preventivamente autorizzati in via generale dall'azienda.

PROCEDURA DA SEGUIRE IN CASO DI VIOLAZIONE DI DATI PERSONALI (DATA BREACH)

Per **"Violazione di dati"** (Data Breach) si intende la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati (art. 4 del GDPR). Qualora si verifichi un incidente di sicurezza il Titolare non risulta essere in grado di garantire il rispetto dei principi prescritti dall'art. 5 del GDPR per il trattamento dei dati personali.

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

Si possono distinguere tre tipi di violazioni:

1. violazione di riservatezza, ovvero quando si verifica una divulgazione o un accesso a dati personali non autorizzato o accidentale;
2. violazione di integrità, ovvero quando si verifica un'alterazione di dati personali non autorizzata o accidentale;
3. violazione di disponibilità, ovvero quando si verifica perdita, inaccessibilità, o distruzione accidentale o non autorizzata di dati personali.

Una singola violazione potrebbe comprendere una o più tipologie.

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

- rischio assente: la notifica al Garante non è obbligatoria;
- rischio presente: la notifica al Garante è necessaria;
- rischio elevato: la notifica al Garante è necessaria in concomitanza alla comunicazione della violazione ai soggetti interessati. Nel momento in cui il Titolare del trattamento ha adottato sistemi di crittografia dei dati e la violazione non ha comportato l'acquisizione della chiave di decrittografia, la comunicazione ai soggetti interessati non è un obbligo.

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

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

La scoperta di un incidente di sicurezza può derivare da diversi soggetti coinvolti, interni e/o esterni all'Istituto:

- dagli autorizzati (personale dipendente, convenzionato, stagisti, tirocinanti, ecc.);
- da parte dei Responsabili esterni del trattamento;
- da parte del DPO;
- da parte degli organi Pubblici (Agid, Polizia, altre Forze dell'Ordine, ecc);
- dai sistemi di monitoraggio automatici dei sistemi informatici;
- dagli interessati e da terzi.

Qualora uno degli autorizzati dovesse rilevare e/o venire a conoscenza di un episodio di violazione ovvero che vi è un rischio serio ed imminente di violazione dei dati personali detenuti, deve procedere ad informare, senza ingiustificato ritardo, il Titolare del trattamento (art. 33 GDPR) e, laddove designato, il Responsabile della Protezione dei Dati (o DPO - Data Protection Officer) inviando opportuna segnalazione tramite messaggio di posta elettronica e/o attraverso i canali comunicativi a tal fine individuati.

RICHIESTE DI ESERCIZIO DEI DIRITTI RICONOSCIUTI ALL'INTERESSATO

Laddove il Titolare elabori dati personali su individui (studenti, genitori, lavoratori, fornitori, etc.) questi possono esercitare i diritti riconosciuti dal GDPR presentando una richiesta al Titolare del trattamento. Gli artt. 11 e 12 del Regolamento disciplinano in linea generale le modalità per l'esercizio di tutti i diritti sorgenti in capo all'interessato.

I diritti che gli interessati possono esercitare includono:

- Diritto di accesso a copia dei dati conservati dal Titolare (art. 15);
- Diritto di rettifica dei dati conservati dal Titolare (art. 16);
- Diritto alla cancellazione ("diritto all'oblio") dei dati conservati dal Titolare (art. 17);
- Diritto alla limitazione delle attività di trattamento da parte del Titolare (art. 18);
- Diritto alla portabilità dei dati dal Titolare ad un'altra entità (art. 20);
- Diritto di opposizione al trattamento effettuato dal Titolare (art. 21);
- Diritto di opposizione al processo decisionale automatizzato effettuato dal Titolare (art. 22).

Se un lavoratore alle dipendenze del Titolare del Trattamento riceve una richiesta di esercizio di un diritto da parte di un lavoratore/cliente/fornitore o altri, la richiesta deve essere immediatamente inviata al soggetto competente insieme all'indicazione della data di ricezione della richiesta e ogni altro dettaglio fornito dal richiedente.

NON OSSERVANZA DELLE PRESENTI ISTRUZIONI

Il mancato rispetto o la violazione delle regole contenute nelle presenti istruzioni è perseguibile da parte del Titolare del trattamento con provvedimenti disciplinari.