INVALSI Istituto nazionale per la valutazione del sistema educativo di istruzione e di formazione
Ente di Diritto Pubblico Decreto Legislativo 286/2004

# DISCIPLINARE PER IL CORRETTO TRATTAMENTO DEI DATI PERSONALI ED ISTRUZIONI ALLE PERSONE AUTORIZZATE AL TRATTAMENTO ANCHE IN RELAZIONE AL CORRETTO UTILIZZO DELLA STRUMENTAZIONE INFORMATICA DELL'ISTITUTO

## RIFERIMENTI NORMATIVI

Il presente documento è elaborato ai sensi delle disposizioni previste da:

- Regolamento EU 2016/679
- Provvedimento Generale del 1 marzo 2007 dell'Autorità Garante in materia di dati personali (Deliberazione n. 13 del 1/3/2007 - pubblicata sulla GU n. 58 del 10 marzo 2007)
- Art. 4 della Legge n. 300/70 come modificato dal Decreto legislativo n. 151/2015

Per quanto qui non previsto si rimanda al Codice Etico di INVALSI.

## OBIETTIVI DEL DOCUMENTO

Il presente documento fornisce una serie di informazioni e istruzioni per il corretto trattamento dei dati personali di cui l'ISTITUTO NAZIONALE PER LA VALUTAZIONE DEL SISTEMA EDUCATIVO DI ISTRUZIONE E FORMAZIONE (nel seguito INVALSI o anche l'Istituto o l'Ente) è Titolare e/o Responsabile del Trattamento e si applica al trattamento interamente o parzialmente automatizzato di dati personali e al trattamento non automatizzato di dati personali contenuti in un archivio o destinati a figurarvi.

Premesso che i comportamenti che normalmente si adottano nell'ambito di un rapporto di lavoro e/o collaborazione, tra i quali rientrano l'utilizzo delle risorse informatiche e telematiche, devono sempre ispirarsi al principio di diligenza e correttezza, INVALSI ha adottato il presente Disciplinare diretto ad evitare che condotte inconsapevoli possano innescare problemi o minacce alla Sicurezza dei dati o delle attrezzature dell'Istituto.

Il presente Disciplinare si pone l'obiettivo di fornire misure di sicurezza e linee di comportamento idonee ad utilizzare in modo conforme e non rischioso gli strumenti di lavoro, la posta elettronica istituzionale e la navigazione in Internet. Si applica ai dipendenti, ai collaboratori e alle persone autorizzate al trattamento che si trovino ad operare con gli strumenti informatici di INVALSI.

Si raccomanda di prestare la massima attenzione nella lettura delle disposizioni di seguito riportate in quanto il rispetto di tali istruzioni, che potranno essere integrate ed aggiornate, è obbligatorio e l'inosservanza delle disposizioni in esso contenute può comportare violazioni della normativa sulla privacy e conseguentemente sanzioni di natura civile e penale, nonché nei confronti dei dipendenti sanzioni di tipo disciplinare e nei confronti dei soggetti esterni risoluzione contrattuale e/o diritto di rivalsa e/o risarcimento dei danni.

## CAMPO DI APPLICAZIONE

Le presenti Istruzioni si applicano:

- a tutti i lavoratori dipendenti e a tutti i collaboratori di INVALSI, a prescindere dal rapporto contrattuale con la stessa intrattenuto (lavoratori somministrati, collaboratori a progetto, agenti, stagisti, consulenti, ecc.) che si trovino ad operare sui dati personali di cui INVALSI stessa sia Titolare;

- a tutte le attività o comportamenti comunque connessi all'utilizzo della rete Internet e della posta elettronica, mediante strumentazione istituzionale o di terze parti autorizzate all'uso dell'infrastruttura istituzionale.

## NORMATIVA DI RIFERIMENTO

Il 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» (di seguito GDPR), ha imposto la previsione ed il rispetto di requisiti, adempimenti formali e misure di sicurezza volti a garantire la tutela dei diritti dell'interessato.

Tale Regolamento, definitivamente vincolante a partire dal 25 maggio 2016, uniforma la normativa in tutti gli Stati Membri e protegge i diritti e le libertà fondamentali delle persone fisiche, in particolare il diritto alla protezione dei dati personali.

## DEFINIZIONI – ART. 4 DEL GDPR

**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.

**Particolari categorie di dati:** dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona (art. 9 del GDPR).

**Dati genetici:** i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione.

**Dati biometrici:** i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici.

**Dati relativi alla salute:** i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute.

**Dati personali relativi a condanne penali e reati**: dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza (art. 10 del GDPR).

**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.

**Limitazione di trattamento:** il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro.

**Profilazione:** qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica.

**Pseudonimizzazione**: il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile.

**Archivio**: qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico.

**Titolare**: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali.

**DPO – Data Protection Officer**: persona designata dal Titolare o dal Responsabile come centro di competenza per il corretto trattamento dei dati personali.

**Responsabile del trattamento**: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratti dati personali per conto del titolare del trattamento.

**Persone autorizzate al trattamento**: le persone fisiche autorizzate, in base a specifiche istruzioni, a compiere operazioni di trattamento dal titolare o dal responsabile. Tali operazioni possono essere effettuate solo da incaricati che operino sotto la diretta autorità del Titolare o del Responsabile, attenendosi alle istruzioni impartite.

**Interessato**: la persona fisica, la persona giuridica, l'ente o l'associazione cui si riferiscono i dati personali.

**Destinatario**: la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica

indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerate destinatari; il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento.

**Terzo**: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile.

**Fiduciario**: altro lavoratore delegato dall'interessato a verificare il contenuto della casella di posta elettronica di quest'ultimo.

**Proxy:** un'applicazione che filtri le informazioni in arrivo da Internet attraverso il firewall; i proxy sono in grado di mantenere traccia di tutte le attività che svolgono.

**File di Log:** la registrazione cronologica delle operazioni, man mano che vengono eseguite, ed anche i file su cui tali registrazioni sono memorizzate.

**Comunicazione**: il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dello Stato, dal responsabile e dagli incaricati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.

**Diffusione**: il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.

**Strumenti elettronici**: gli elaboratori, i programmi per elaboratori e qualunque dispositivo elettronico o comunque automatizzato con cui si effettua il trattamento.

**Violazione dei dati personali - Data breach:** Violazione di sicurezza che comporti 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.

**Autorità di controllo**: l'autorità pubblica indipendente istituita da uno Stato membro.

## PRINCIPI APPLICABILI AL TRATTAMENTO DEI DATI PERSONALI

Ai sensi dell'art. 5 del GDPR, i dati personali oggetto di trattamento sono:

- trattati in modo lecito e secondo correttezza **(Liceità, correttezza e trasparenza)**;

- raccolti e registrati unicamente per finalità istituzionali, esplicite e legittime, e successivamente trattati in modo tale che il trattamento non sia incompatibile con tali finalità; un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è considerato incompatibile con le finalità iniziali ("**limitazione della finalità**");
- adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati ("**minimizzazione dei dati**");
- esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati ("**esattezza**");
- conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, fatta salva l'attuazione di misure tecniche e organizzative adeguate a tutela dei diritti e delle libertà dell'interessato ("**limitazione della conservazione**");
- trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali ("**integrità e riservatezza**").

## LINEE GUIDA GENERALI

Di seguito vengono descritte le norme a cui le persone autorizzate al trattamento devono attenersi nell'esecuzione dei compiti che implicano un trattamento di dati personali. Al fine di evitare che soggetti estranei possano venire a conoscenza dei dati personali, la persona autorizzata deve osservare le seguenti regole di ordinaria diligenza, nonché tutte le altre ulteriori misure ritenute necessarie per garantire il rispetto di quanto disposto dalla normativa in ambito privacy:

- tutte le operazioni di trattamento devono essere effettuate in modo tale da garantire il rispetto delle misure di sicurezza, la massima riservatezza delle informazioni di cui si viene in possesso considerando tutti i dati confidenziali e, di norma, soggetti al segreto d'ufficio;
- le singole fasi di lavoro e la condotta da osservare devono consentire di evitare che i dati siano soggetti a rischi di perdita o distruzione, che vi possano accedere persone non autorizzate, che vengano svolte operazioni di trattamento non consentite o non conformi ai fini per i quali i dati stessi sono stati raccolti;
- in caso di allontanamento, anche temporaneo, dalla propria postazione di lavoro si devono porre in essere tutte le misure necessarie (es. blocco del pc) affinché soggetti terzi, anche se dipendenti, non possano accedere ai dati personali per i quali era in corso un qualunque tipo di trattamento, sia esso cartaceo che automatizzato;
- non devono essere eseguite operazioni di trattamento per fini non previsti tra i compiti assegnati dal diretto responsabile;
- devono essere svolte le sole operazioni di trattamento necessarie per il raggiungimento dei fini per i quali i dati sono stati raccolti;
- deve essere costantemente verificata l'esattezza dei dati trattati e la pertinenza rispetto alle finalità perseguite nei singoli casi.

Quanto sopra descritto impone, in altri termini, di operare con la massima attenzione in tutte le fasi di trattamento, dalla esatta acquisizione dei dati, al loro aggiornamento, alla conservazione ed eventuale distruzione.

## ISTRUZIONI COMPORTAMENTALI E MISURE DI SICUREZZA

**Accesso ai dati.**

I dati personali cui è consentito accedere sono quelli la cui conoscenza è strettamente necessaria per adempiere ai compiti affidati, indispensabili per l'esecuzione della prestazione. Ogni variazione ai diritti di accesso al momento detenuti, sarà opportunamente comunicata di volta in volta.
Le persone autorizzate possono effettuare esclusivamente i trattamenti di dati personali definiti per iscritto e comunicati all'atto della designazione, con la conseguente possibilità di accesso ed

utilizzo della documentazione cartacea, degli strumenti informatici, e delle banche dati istituzionali che contengono i predetti dati personali.

**Accesso ai dati dalla postazione di lavoro.**

La postazione di lavoro deve essere:

- utilizzata solo per scopi legati alla propria attività lavorativa;
- utilizzata in modo esclusivo da un solo utente;
- protetta, evitando che terzi possano accedere ai dati che si stanno trattando.

È dovere della persona autorizzata al trattamento:

- non utilizzare c/o l'Istituto risorse informatiche private se non autorizzate (PC, periferiche, token, ecc.);
- non installare sui dispositivi dell'Istituto alcun software;
- non lasciare sulla scrivania informazioni riservate su qualunque supporto esse siano archiviate (carta, CD, dischetti, ecc.);
- richiamare le funzioni di sicurezza del sistema operativo (con la sequenza dei tasti CTRL+ALT+CANC) ed assicurarsi della attivazione della funzione Lock Workstation in caso di abbandono momentaneo del proprio PC;
- non lasciare il computer portatile incustodito sul posto di lavoro (al termine dell'orario lavorativo, durante le pause di lavoro o durante riunioni lontane dalla propria postazione);
- non lasciare incustoditi cellulari e palmari;
- non utilizzare fax e/o telefono per trasmettere informazioni riservate e personali se non si è assolutamente certi dell'identità dell'interlocutore o del destinatario e se esso non è legittimato a riceverle.

**Trattamento.**

Il trattamento deve essere effettuato esclusivamente:

- nel rispetto delle istruzioni ricevute dal Titolare;
- in conformità alle finalità previste e dichiarate dall'Istituto e alle informazioni che l'Istituto ha comunicato agli interessati;
- in modo lecito e secondo correttezza;
- con particolare attenzione all'esattezza dei dati trattati, provvedendo tempestivamente, se di propria competenza, all'aggiornamento degli stessi;

- con assoluto riserbo sui dati personali di cui si venga a conoscenza nell'esercizio delle proprie funzioni.

Senza la preventiva autorizzazione del Titolare non è permesso realizzare nuove ed autonome banche dati contenenti dati personali, secondo criteri organizzativi e/o per finalità diverse da quelle già previste.

**Raccolta dei dati.**

All'atto della raccolta dei dati, il personale autorizzato al trattamento deve fornire all'interessato l'informativa sul trattamento dei dati personali, avendo cura di raccogliere il suo consenso, attraverso i moduli di informativa e consenso predisposti da INVALSI. Per tale modulistica occorre rivolgersi al Titolare del trattamento e/o delegato privacy dell'Istituto.

Qualora per esigenze legate alla sua mansione ritenga necessario effettuare un trattamento diverso rispetto a quello riportati nell'informativa agli interessati, sotto il profilo dei dati trattati, delle finalità, dell'ambito di comunicazione o diffusione, dovrà consultare preventivamente il Titolare del trattamento e/o il delegato privacy dell'Istituto al fine di individuare la necessità del trattamento medesimo e degli obblighi conseguenti.

**Riservatezza delle informazioni.**

Occorre prestare molta attenzione alla riservatezza delle informazioni scambiate e alla custodia dei dati al fine di garantirne l'integrità, la disponibilità e la riservatezza.

- Nessuna informazione riservata, in particolare quelle contenenti dati personali, può essere condivisa con personale non autorizzato, interno o esterno.
- Il trattamento dei dati da parte delle persone autorizzate al trattamento è vincolato al rispetto del segreto d'ufficio.
- Il vincolo di riservatezza è valido anche una volta terminato il trattamento dei dati personali e/o il rapporto di lavoro dipendente e/o di consulenza.

**Attività al computer.**

Hanno diritto all'utilizzo degli strumenti e ai relativi accessi solo i dipendenti e collaboratori che per funzioni lavorative ne abbiano un effettivo e concreto bisogno. Il computer in dotazione al dipendente e/o collaboratore 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, costi di manutenzione e, soprattutto minacce alla sicurezza. L'utilizzo del computer deve prevedere quindi precisi accorgimenti al fine di impedire accessi alle informazioni da parte di persone non autorizzate. In particolare è richiesto di:

- utilizzare solo ed esclusivamente le aree di memoria della Rete di INVALSI, ed ivi creare e registrare file e software o archivi dati, senza pertanto creare altri files fuori dalle unità di Rete;
- mantenere sul computer esclusivamente i dispositivi di memorizzazione, comunicazione o altro (come ad esempio masterizzatori, modem, ecc.), disposti da INVALSI;
- attivare la schermata di protezione (screensaver con password) del PC quando ci si allontana momentaneamente dalla propria postazione di lavoro (casa o ufficio);
- spegnere il terminale a fine lavoro o mettere in modalità "Standby";
- non rimuovere o aggiungere alcuna apparecchiatura o componente della stazione di lavoro, salvo specifica autorizzazione;
- non registrare alcun file, software o archivio dati nel disco fisso o memoria di massa del computer in dotazione;
- non modificare le configurazioni già impostate sul personal computer;
- non utilizzare programmi e/o sistemi di criptazione senza la preventiva autorizzazione scritta;
- non installare alcun software di cui INVALSI 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 di INVALSI. Né è, peraltro, consentito fare copia del software installato al fine di farne un uso personale;
- non caricare sul disco fisso del computer alcun documento, gioco, file musicale o audiovisivo o immagine diversi da quelli necessari allo svolgimento delle mansioni affidate;
- non aggiungere o collegare dispositivi hardware (ad esempio hard disk, driver, PCMCIA, ecc.) o periferiche (telecamere, macchine fotografiche, chiavi USB ecc.) diversi da quelli consegnati, senza espressa autorizzazione;

- non creare o diffondere, intenzionalmente o per negligenza, programmi idonei a danneggiare il sistema informatico di INVALSI, quali per esempio virus, trojan horses ecc.;
- non accedere, rivelare o utilizzare informazioni non autorizzate o comunque non necessarie per le mansioni svolte;
- non copiare dati sensibili sulla propria stazione di lavoro, se non previamente autorizzato.

**Protezione dei PC portatili e cellulari**

Il computer portatile e il cellulare possono venire concessi in uso da INVALSI alle persone autorizzate al trattamento che durante gli spostamenti necessitino di disporre di archivi elettronici, supporti di automazione e/o di connessione alla rete di INVALSI. Il dipendente è responsabile del PC portatile e degli altri dispositivi elettronici assegnatigli e deve custodirli con diligenza sia durante gli spostamenti che durante l'utilizzo nel luogo di lavoro.

Un computer portatile presenta maggiori vulnerabilità rispetto ad una postazione di lavoro fissa. Fatte salve tutte le disposizioni dei paragrafi precedenti, di seguito vengono illustrate le ulteriori precauzioni da adottare nell'uso dei dispositivi portatili:

- conservare lo strumento in un luogo sicuro alla fine della giornata lavorativa;
- non lasciare mai incustodito l'elaboratore in caso di utilizzo in ambito esterno all'Istituto;
- avvertire tempestivamente l'Area IT, che darà le opportune indicazioni, in caso di furto di un PC portatile o di un cellulare;
- essere sempre ben consapevole delle informazioni archiviate sul portatile o sul cellulare istituzionale, che sono maggiormente soggetti a furto e smarrimento rispetto alla postazione fissa;
- operare sempre nella massima riservatezza quando si utilizza il PC portatile o il cellulare in pubblico: i dati, ed in particolare le password, potrebbero essere intercettati da osservatori indiscreti.

Al dipendente non è permesso svolgere la sua attività su cellulari, PC fissi o portatili personali se non autorizzato.

**Utenza e password.**

L'accesso all'elaboratore è protetto da password che deve essere custodita dalla persona autorizzata al trattamento con la massima diligenza e non divulgata. In particolare quest'ultima deve gestire la propria utenza d'accesso ai sistemi e la propria password rispettando le seguenti regole:

- L'utenza e la password devono essere utilizzate in maniera individuale, strettamente personale e riservata, senza condividerle con altre persone. È vietato permettere ad altri utenti (es. colleghi) di operare con il proprio identificativo utente.
- La password rilasciata in maniera provvisoria per permettere di accedere per la prima volta al sistema deve essere modificata immediatamente al primo utilizzo.

Successivamente, ove non sia già imposto da sistema, la password deve essere gestita secondo le seguenti regole:

- deve contenere sia lettere che numeri e almeno un carattere maiuscolo, essere lunga almeno 8 caratteri o, nel caso in cui lo strumento elettronico non lo consenta, un numero di caratteri pari al massimo consentito;
- deve essere diversa dalle 5 utilizzate in precedenza;
- deve essere difficilmente riconducibile all'utente (ad es. non utilizzare il nome, il cognome etc..) e non deve essere ovvia (ad es. non il nome dell'ufficio, dei figli, ecc.);
- deve essere conservata, se memorizzata, in luoghi non visibili (ad es. evitare "memo" attaccati al video, al calendario o alla lavagna dell'ufficio, etc.), non ovvi (ad es. non nell'agenda, nel primo cassetto etc.) e non deve mai essere memorizzata sul proprio PC;
- deve essere cambiata almeno ogni 6 mesi (3 mesi nell'eventualità di accesso a dati sensibili) ed immediatamente nel caso in cui sorga il minimo dubbio circa la sua conoscenza da parte di altri utenti;
- non deve mai essere comunicata per telefono e tantomeno via posta elettronica, salvo gravi necessità.

L'utenza è personale ed univoca nel tempo. Deve essere revocata nel caso in cui venga meno la necessità di accedere al sistema e disattivata in caso di inattività per oltre 6 mesi.

**Protezione dai virus informatici:** I Personal Computer (PC) in dotazione, pur protetti contro gli attacchi dei virus informatici mediante appositi programmi, rimangono potenzialmente esposti ad aggressioni di virus informatici non conosciuti. Alcuni di questi consentono di estrapolare informazioni dal proprio computer (es. utenze e password) e per ridurre le probabilità del verificarsi di tali attacchi è necessario che vengano osservate le seguenti regole:

- non disinstallare né modificare il software antivirus;
- verificare che il programma antivirus installato sia attivo ed aggiornato, in caso contrario segnalare la necessità di aggiornamento;
- chiudere correttamente i programmi in uso;
- non utilizzare CD-Rom o altri supporti elettronici di provenienza incerta e verificare con l'ausilio del programma antivirus in dotazione ogni supporto magnetico contenente dati (floppy disk o CD-Rom), prima dell'esecuzione dei file in esso contenuti;
- assicurarsi, prima dell'accensione o di un riavvio del sistema operativo, che nessun supporto magnetico (floppy, CD-Rom, ecc.) sia inserito nell'apposita unità;
- non operare modifiche alla configurazione degli strumenti informatici in dotazione senza l'autorizzazione del personale preposto. È vietato modificare le caratteristiche impostate sulle dotazioni od installare dispositivi di memorizzazione, comunicazione o altro (ad esempio masterizzatori, modem, wi-fi o connect card), collegare alla rete istituzionale qualsiasi apparecchiatura (ad es. switch, hub, apparati di memorizzazione di rete, ecc.), effettuare collegamenti verso l'esterno di qualsiasi tipo (ad es. tramite modem o connect card ecc.) utilizzando un pc che sia contemporaneamente collegato alla rete INVALSI (creando così un collegamento tra la rete istituzionale interna e la rete esterna);
- non aprire, se si lavora in rete, files sospetti e di dubbia provenienza e non installare applicazioni o software non autorizzato;
- porre la necessaria attenzione sui risultati delle elaborazioni effettuate e sulle eventuali segnalazioni anomale inviate dal PC e nel caso in cui il sistema rilevi la presenza di un virus sulla stazione di lavoro contattare immediatamente il personale di competenza;
- usare correttamente e solo per esigenze di lavoro i servizi di posta elettronica ed Internet e spegnere il PC al termine della giornata di lavoro.

**Restituzione dei Device**

A seguito della cessazione del rapporto lavorativo o di consulenza con l'organizzazione o, comunque, al venir meno, ad insindacabile giudizio dell'ente, della permanenza dei presupposti per l'utilizzo dei device istituzionali, gli utilizzatori hanno i seguenti obblighi:

a. procedere immediatamente alla restituzione dei device in uso;

b. divieto assoluto di formattare o alterare o manomettere o distruggere i device assegnati o rendere inintelligibili i dati in essi contenuti tramite qualsiasi processo.

**Backup.**

I dati inseriti nei sistemi devono essere salvati con frequenza al più settimanale o comunque commisurata alla frequenza di aggiornamento degli stessi.

**Utilizzo di Internet.**

Gli strumenti di comunicazione telematica (Internet e Posta elettronica) devono essere utilizzati solo ed esclusivamente per finalità lavorative, consapevoli del fatto che si tratti di veicoli per l'introduzione sulla propria macchina (e quindi in INVALSI) di virus e altri elementi potenzialmente dannosi.

Sono vietati comportamenti che possano arrecare danno all'ISTITUTO. La navigazione deve essere effettuata in modo etico e solo al fine di migliorare la propria produttività. In particolare, è necessario osservare le seguenti regole:

- È consentita la navigazione internet solo in siti attinenti e necessari per lo svolgimento delle mansioni assegnate.
- 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.
- È consentito solo l'utilizzo dei programmi ufficialmente installati dall'Area IT, mentre è assolutamente vietato sia scaricare software gratuiti (freeware o shareware) prelevati da siti Internet che installare autonomamente programmi, per ovviare al grave pericolo di

introdurre virus informatici e/o di alterare la funzionalità delle applicazioni software esistenti e/o di violare la legge sul diritto d'autore, non disponendo delle apposite licenze d'uso acquistate da INVALSI.

- È vietata ogni forma di registrazione a siti, la partecipazione a Forum non professionali, l'utilizzo di chat line, di bacheche elettroniche i cui contenuti non siano legati all'attività lavorativa.
- Non è consentito l'utilizzo funzioni di instant messaging a meno che non siano state autorizzate dall'Area IT.
- Salva esplicita autorizzazione in tal senso, è vietata la comunicazione di dati personali attraverso l'uso di telefoni cellulari, smatphone, tablet e pc personali.
- È vietata la diffusione sui social network di immagini del luogo nel quale si svolge l'attività lavorativa.
- 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.
- È vietato al lavoratore utilizzare la rete internet istituzionale per condurre attività di business personali.
- È vietato creare siti web personali sui sistemi di INVALSI nonché acquistare beni o servizi su Internet a meno che l'articolo acquistato non sia stato approvato a titolo di spesa professionale.
- È vietato accedere ad alcuni siti internet mediante azione inibenti dei filtri, sabotando o comunque superando o tentando di superare o disabilitando i sistemi adottati per bloccare accessi non conformi all'attività lavorativa. In ogni caso è vietato utilizzare siti o altri strumenti che realizzino tale fine.
- Le persone autorizzate al trattamento sono tenute al rispetto della regolamentazione del copyright (es. legge 22 aprile 1941, n. 633 e successive modificazioni, d.lgs. 6 maggio 1999, n. 169 e legge 18 agosto 2000, n. 248) anche per i programmi freeware e shareware scaricati dalla rete; ciò deve valere anche per lo scarico di materiale mediatico (es. immagini, mp3, …).

- Non devono essere messi a disposizione materiali a carattere inappropriato od offensivo, ed è comunque vietato accedervi.
- Non devono essere messe a disposizione di terzi informazioni a carattere riservato o personale.
- Ogni eventuale navigazione di questo tipo comportando un illegittimo utilizzo di Internet, nonché un possibile illecito trattamento di dati personali e sensibili è posta sotto la personale responsabilità della persona autorizzata inadempiente.

**Social Media**

Con specifico riferimento ai Social Media si precisa che non è consentito l'accesso a tali Social Media per motivi personali durante l'orario di lavoro.

Per motivi legati al lavoro l'accesso a tali Social Media sarà consentito attenendosi al presente disciplinare.
In ogni caso tutte le iniziative di social media che coinvolgono o fanno riferimento ad INVALSI devono essere preventivamente autorizzate dalla Direzione.
Solo un portavoce ufficialmente nominato potrà comunicare per conto di INVALSI nell'ambito dei Social Media.

**Posta elettronica.**

La posta elettronica è uno strumento a disposizione per l'attività lavorativa e deve essere utilizzato nel rispetto dell'etica e dell'immagine di INVALSI

- La posta elettronica e qualsiasi altro strumento di connessione telematica deve essere utilizzato nel rispetto delle norme civili e penali vigenti e per scopi compatibili con le attività istituzionali.
- In INVALSI le persone autorizzate al trattamento hanno l'utilizzo di indirizzi nominativi di posta elettronica salvo specifiche e determinate eccezioni (indirizzi istituzionali).
- Le persone assegnatarie delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse.

- Prestare attenzione ai messaggi di posta elettronica ed ai file, programmi e oggetti allegati, ricevuti da mittenti sconosciuti, con testo del messaggio non comprensibile o comunque avulso dal proprio contesto lavorativo. In tali casi le persone autorizzate al trattamento devono in particolare:

  - visualizzare preventivamente il contenuto tramite utilizzo della funzione "Riquadro di lettura" (o preview) e, nel caso si riscontri un contenuto sospetto, non aprire il messaggio,

  - una volta aperto il messaggio, evitare di aprire gli allegati o cliccare sui "link" eventualmente presenti,

  - cancellare il messaggio e svuotare il "cestino" della posta,

  - segnalare l'accaduto all'Amministratore di Sistema.

- Non è consentito rispondere a messaggi provenienti da un mittente sconosciuto o di dubbio contenuto in quanto tale atto assicura al mittente l'esistenza del destinatario.
- È vietato l'utilizzo della posta elettronica per comunicare informazioni riservate, dati personali o dati critici, senza garantirne l'opportuna protezione.
- Occorre sempre accertarsi che i destinatari della corrispondenza per posta elettronica siano autorizzati ad entrare in possesso dei dati che ci si appresta ad inviare.
- Al fine di ottimizzare le risorse a disposizione della posta elettronica istituzionale e migliorare le prestazioni del sistema si evidenzia che la casella di posta deve essere "tenuta in ordine" cancellando periodicamente o comunque se sono superati i limiti di spazio concessi, documenti inutili o allegati ingombranti.

**Particolari cautele nella predisposizione dei messaggi di posta elettronica.**

Nell'utilizzo della posta elettronica ogni persona autorizzata al trattamento deve tenere in debito conto che i soggetti esterni possono attribuire carattere istituzionale alla corrispondenza ricevuta da dipendenti. Pertanto si deve prestare particolare attenzione agli eventuali impegni contrattuali e precontrattuali contenuti nei messaggi e rispettare le seguenti prescrizioni in proposito:

- La formulazione dei messaggi deve prevedere l'uso di un linguaggio appropriato, corretto e rispettoso, che tuteli la dignità delle persone, l'immagine e la reputazione dell'Istituto.

- Devono essere conservate le comunicazioni inviate o ricevute, in particolare quelle dalle quali si possano desumere impegni e/o indicazioni operative provenienti dalla Committenza pubblica.
- Evitare di cliccare sui collegamenti ipertestuali dubbi presenti nei messaggi di posta: in caso di necessità, accedere ai siti segnalati digitando il nome del sito da visitare direttamente nella barra degli indirizzi nei consueti strumenti di navigazione.
- È vietato utilizzare l'indirizzo di posta elettronica contenente il dominio di INVALSI per iscriversi in qualsivoglia sito per motivi non attinenti all'attività lavorativa, senza espressa autorizzazione scritta di INVALSI, nonché utilizzare il dominio istituzionale per scopi personali.
- In caso di iscrizione a servizi informativi accessibili via internet ovvero a servizi di editoria on line necessari per lo svolgimento dell'attività professionale, veicolati attraverso lo strumento di posta elettronica:

  - adoperare estrema cautela ed essere selettivi nella scelta della società che fornisce il servizio (in particolare, l'adesione dovrà avvenire in funzione dell'attinenza del servizio con la propria attività lavorativa);

  - utilizzare il servizio solo per acquisire informazioni inerenti finalità istituzionali, facendo attenzione alle informazioni fornite a terzi in modo da prevenire attacchi di social engineering.
- In caso di errore nella spedizione o ricezione, contattare rispettivamente il destinatario cui è stata trasmessa per errore la comunicazione o il mittente che, per errore, l'ha spedita, eliminando quanto ricevuto (compresi allegati) senza effettuare copia.
- Evitare di predisporre messaggi che contengano materiali in violazione della legge sul diritto d'autore, o altri diritti di proprietà intellettuale o industriale.
- Non è permesso lo scambio di messaggi in conflitto con l'etica professionale o con gli interessi di INVALSI.
- È vietato redigere messaggi di posta elettronica utilizzando l'indirizzo istituzionale, diretti a destinatari esterni, senza utilizzare il seguente disclaimer:

  *«Il presente messaggio e gli eventuali allegati sono di natura istituzionale e prevalentemente confidenziale: qualora vi fosse pervenuto per errore, vi*

*preghiamo di cancellarlo dal vostro sistema. 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 soggetti appartenenti a* INVALSI *per finalità di sicurezza informatica, amministrative e allo scopo del continuo svolgimento dell'attività istituzionale".*

- È vietato l'utilizzo della posta elettronica istituzionale per condurre attività di business personali.
- È vietato creare, archiviare o spedire, anche solo all'interno della rete istituzionale, 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 istituzionale.
- È vietato utilizzare il servizio di posta elettronica per trasmettere a soggetti esterni a INVALSI informazioni riservate o comunque documenti istituzionali, se non nel caso in cui ciò sia necessario in ragione delle mansioni svolte.
- È vietato inviare, tramite la posta elettronica, anche all'interno della rete istituzionale, materiale a contenuto violento, sessuale o comunque offensivo dei principi di dignità personale, di libertà religiosa, di libertà sessuale o di manifestazione del pensiero, anche politico.
- È vietato inviare messaggi di posta elettronica, anche all'interno della rete istituzionale, 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, dello stato di salute.
- Qualora il dipendente riceva messaggi aventi tale contenuto, è tenuto a cancellarli immediatamente e a darne comunicazione alla Direzione.
- Il collaboratore ha l'obbligo di attivare il servizio di risposta automatica (Auto-reply), in caso di assenze programmate e non programmata. In tale ultimo caso qualora il collaboratore non possa attivare il servizio ha l'obbligo di segnalarne la necessità.

**Comunicazione di dati personali e trasmissione di documenti.**

I dati personali potranno circolare regolarmente tra tutti i dipendenti **che ne abbiano necessità per esigenze di lavoro** e che siano già stati autorizzati al trattamento dei dati personali. Peraltro qualsiasi dato personale a cui Lei ha accesso non potrà essere trasmesso a terzi, se non per finalità istituzionali e previa autorizzazione del Titolare o del Responsabile del Trattamento se designato.

In caso di trasmissione o comunicazione di documenti contenenti dati personali necessaria per lo svolgimento dei suoi compiti, al fine di prevenire eventuali accessi ai dati istituzionali da parte di soggetti terzi non autorizzati, occorre adottare le seguenti cautele:

1) Quando le informazioni devono essere trasmesse telefonicamente occorre essere assolutamente certi dell'identità dell'interlocutore e verificare che esso sia legittimato ad ottenere quanto domandato. In particolare, nel caso di richieste da parte di terzi può essere necessario, a seconda della natura dei dati richiesti, procedere nel seguente modo:

• chiedere il nome del chiamante e la motivazione della richiesta;

• richiedere il numero di telefono da cui l'interlocutore sta effettuando la chiamata;

• verificare che il numero dichiarato corrisponda a quello del chiamante;

• procedere immediatamente a richiamare la persona che ha richiesto l'informazione, con ciò accertandosi della identità dichiarata in precedenza;

• non lasciare nella memoria della segreteria telefonica messaggi relativi a dati personali.

2) Quando il dato deve essere inviato a mezzo fax, posta elettronica o SMS, occorre:

• prestare la massima attenzione affinché il numero telefonico o l'indirizzo e-mail immessi siano corretti;

• verificare che non vi siano inceppamenti di carta o che dalla macchina non siano presi più fogli e attendere sempre il rapporto di trasmissione per un ulteriore verifica del numero del destinatario e della quantità di pagine inviate;

• nel caso di documenti inviati per posta elettronica accertarsi, prima di confermare l'invio, di avere allegato il file giusto;

• in caso di trasmissione di dati particolarmente delicati è opportuno anticipare l'invio chiamando il destinatario della comunicazione al fine di assicurare il ricevimento nelle mani del medesimo, evitando che terzi estranei o non autorizzati conoscano il contenuto della documentazione inviata.

**Archivi cartacei e riproduzione di copie cartacee**

Nel caso di accesso e trattamento di dati personali su supporti di tipo cartaceo, la persona autorizzata è tenuta a custodirli con diligenza, non disperderli, e riporli negli appositi contenitori dopo l'uso, avendo cura di chiuderli a chiave. È tenuto a custodirli fino alla restituzione, in modo da evitare l'accesso agli stessi dati da parte di persone prive di autorizzazione.

In caso di trattamento di dati particolarmente sensibili (condizione di salute, dati giudiziari, ecc.), tutta la documentazione cartacea deve essere conservata in armadi/cassetti chiusi a chiave o stanze chiuse a chiave e le chiavi devono essere custodite con cura. L'accesso a tutti i locali deve essere consentito solo a personale preventivamente autorizzato dal Titolare.

I documenti, o copia degli stessi, non possono essere portati fuori dai luoghi di lavoro senza specifica autorizzazione, salvo i casi di comunicazione dei dati a terzi preventivamente autorizzati in via generale dall'Ente.

Tutto il materiale cartaceo contenente dati personali non deve essere lasciato incustodito sulle scrivanie e, a fine lavoro o durante le pause prolungate, deve essere riposto in un luogo sicuro. Inoltre, occorre usare la medesima perizia nello svolgimento delle normali quotidiane operazioni di lavoro, per evitare che il materiale risulti facilmente visibile a persone terze o, comunque, ai non autorizzati al trattamento.

- Non è consentito effettuare stampe o fotocopie di documenti contenenti dati personali se non necessario. Nel caso sia necessario effettuare una stampa, utilizzare apparecchiature collocate in aree controllate. Quando non disponibili, presidiarle in fase di stampa.
- Tutti coloro che provvedono alla duplicazione di documenti con stampanti, macchine fotocopiatrici o altre apparecchiature, in caso di copia erronea o non leggibile correttamente, da cui potrebbero essere desunti dati personali, sono tenuti a distruggere il documento mediante apposita macchina "distruggi documenti" o con qualunque altro mezzo che ne renda impossibile la ricostruzione in modo da escludere qualunque possibilità da parte di estranei di venire a conoscenza dei dati medesimi.

- Procedere in ogni caso alla cancellazione/distruzione secondo le modalità sopra descritte delle copie di dati appena non siano più necessarie, al fine di evitare la proliferazione incontrollata di archivi contenenti dati personali.
- Non lasciare incustoditi i documenti contenenti dati personali nella fotocopiatrice, sul fax, nella stampante.
- Formattare i supporti informatici removibili quando i dati personali ivi salvati non sono più necessari, oppure renderli non più utilizzabili.

**Data Breach:** Nel caso in cui la persona autorizzata al trattamento venga a conoscenza di una violazione dei dati personali (data breach) deve provvedere ad informare senza ritardo il Titolare affinché possa notificare la violazione all'autorità di controllo competente, secondo quanto previsto dall'articolo 33 del GDPR.

**Accesso ai dati da parte dell'Amministratore di Sistema**

L'Amministratore di Sistema può accedere ai dati trattati tramite posta elettronica o navigazione in rete esclusivamente per motivi di sicurezza e protezione del sistema informatico (ad es., contrasto virus, malware, intrusioni telematiche, fenomeni quali spamming, phishing, spyware, etc.), ovvero per motivi tecnici e/o manutentivi e/o di regolare svolgimento dell'attività lavorativa (ad esempio aggiornamento/sostituzione/implementazione di programmi, manutenzione hardware). Fatta eccezione per gli interventi urgenti che si rendano necessari per affrontare situazioni di emergenza e massima sicurezza, il personale incaricato accederà ai dati su richiesta della persona autorizzata al trattamento e/o previo avviso al medesimo.

Ove sia necessario per garantire la sicurezza, l'assistenza tecnica e la normale attività operativa, il personale incaricato avrà anche la facoltà di collegarsi e visualizzare in remoto il desktop delle singole postazioni. Lo stesso Amministratore di Sistema può, nei casi suindicati, procedere a tutte le operazioni di configurazione e gestione necessarie a garantire la corretta funzionalità del sistema informatico istituzionale (ad es. rimozione di file o applicazioni pericolosi).

Può capitare, che INVALSI debba conoscere il contenuto dei messaggi di posta elettronica in caso di assenza improvvisa del destinatario e per improrogabili necessità legate all'attività lavorativa.

A tale scopo ciascun dipendente dovrà designare preventivamente un proprio fiduciario tra i colleghi di lavoro e comunicarlo al Responsabile dei Servizi Informatici

Il responsabile gerarchico del dipendente assente deve manifestare al Responsabile dei servizi informatici la necessità di accedere alla relativa casella di posta elettronica.

Il Responsabile dei servizi informatici allora renderà disponibile al fiduciario del dipendente assente la casella di posta elettronica tramite la creazione di una password temporanea. Al rientro, l'utente assente verrà avvisato dell'operazione di cui sopra e dovrà modificare la propria password.

Il verbale di tali operazioni è riservato ed è conservato a cura del Responsabile dei servizi informatici

L'Amministratore di Sistema può procedere a controlli sulla navigazione finalizzati 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.

L'eventuale controllo sui file di log da parte dell'Amministratore di Sistema non è comunque continuativo ed è limitato ad alcune informazioni (es. Posta elettronica: l'indirizzo del mittente e del destinatario, la data e l'ora dell'invio e della ricezione e l'oggetto –Navigazione Internet: il nome dell'utente, l'identificativo della postazione di lavoro, indirizzo IP, la data e ora di navigazione, il sito visitato e il totale degli accessi effettuati) ed i file stessi vengono conservati per il periodo strettamente necessario per il perseguimento delle finalità organizzative, produttive e di sicurezza dell'Istituto, e comunque non oltre 12 mesi, fatti salvi in ogni caso specifici obblighi di legge.

Il sistema di registrazione dei log è configurato per cancellare periodicamente ed automaticamente (attraverso procedure di sovraregistrazione) i dati personali degli utenti relativi agli accessi internet e al traffico telematico.

L'Amministratore di Sistema è altresì abilitato ad accedere ai dati contenuti negli strumenti informatici restituiti dal dipendente o collaboratore all'Istituto per cessazione del rapporto, sostituzione delle apparecchiature, etc.

Sarà cura dell'utente la cancellazione preventiva di tutti gli eventuali dati personali eventualmente ivi contenuti.

In ogni caso, INVALSI 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 (log) al di là di quanto tecnicamente necessario per svolgere il servizio e-mail;

• riproduzione ed eventuale memorizzazione sistematica delle pagine web visualizzate dal lavoratore;

• lettura e registrazione dei caratteri inseriti tramite la tastiera o analogo dispositivo.

**MODALITÀ DI CONTROLLO E VERIFICA.**

Il costante processo di informatizzazione consente alle organizzazioni di poter rendere disponibili ai collaboratori strumenti di lavoro informatici, il cui scorretto utilizzo può gravemente nuocere all'interesse del datore di lavoro.

La progressiva diffusione delle nuove tecnologie informatiche ed in particolare l'accesso alla rete internet dal computer dell'Ente espone il medesimo Ente a possibili rischi di un coinvolgimento di rilevanza sia civile, sia penale, sia amministrativa, creando problemi alla sicurezza e all'immagine dell'organizzazione stessa

L'abuso della casella postale informatica assegnata al dipendente e gli accessi ad Internet per finalità extra-lavorative, possono infatti provocare danni all'organizzazione non solo come perdita di risorse lavorative, ma anche in termini di danni provocati dall'illecita o incauta attività svolta dal lavoratore.

Anche l'utilizzo improprio delle apparecchiature telefoniche messe a disposizione del lavoratore può risultare dannoso in termini di risorse per l'organizzazione.

Dall'altra parte, la tecnologia informatica potrebbe permettere potenzialmente al datore di lavoro di poter verificare con precisione ogni utilizzo improprio degli strumenti informatici, "registrando" ogni connessione alla rete, consentendo inoltre di verificare il flusso di posta in entrate ed in uscita di ogni singola postazione di lavoro, nonché l'indirizzo dei siti visitati dallo stesso.

La possibilità di usufruire efficacemente di tali forme di controllo si scontra, però, con la copiosa normativa che disciplina specificamente il rapporto di lavoro e, in generale, la tutela della riservatezza.

La materia è stata di recente ridisciplinata con la modifica dell'art. 4 della Legge n. 300/70 – Statuto dei lavoratori – attuata dal Decreto Legislativo n. 151/2015 del 24.09.2015. Detto Decreto Legislativo 151/2015 da un lato lascia invariata la previgente regola per cui gli impianti audiovisivi e gli altri strumenti, dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori, possono essere impiegati esclusivamente per esigenze organizzative e produttive, per la sicurezza sul lavoro e per la tutela del patrimonio dell'Ente, previo accordo con le rappresentanze sindacali, od in mancanza di detto accordo, previo ottenimento della autorizzazione della Direzione territoriale del lavoro.

Dall'altro lato prevede che la suddetta disposizione non si applica agli strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa e agli strumenti di registrazione degli accessi e delle presenze.

In ogni caso detto Decreto Legislativo 151/2015 prevede che le informazioni raccolte con gli strumenti di cui sopra, possano essere utilizzate ai fini connessi al rapporto di lavoro a condizione che sia data al lavoratore adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli e nel rispetto di quanto previsto dalla normativa sulla protezione dei dati personali, da ultimo disciplinata dal Regolamento EU 2016/679.

Le regole dettate in materia dalla legge sulla privacy sono arricchite dal Provvedimento Generale del 1 marzo 2007, Linee guida del Garante per la posta elettronica e Internet con il quale il Garante per la protezione dei dati personali impone ai datori di lavoro di definire le modalità d'uso di tali strumenti.

Nonché, per il settore pubblico, dalle "Linee guida in materia di trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro in ambito pubblico" - 14 giugno 2007 (G.U. 13 luglio 2007, n. 161)

Anche per fare fronte ai suddetti obblighi, INVALSI nel pieno rispetto di quanto previsto dal nuovo articolo 4 della Legge n. 300/70, dal Regolamento EU 2016/679 e dal Provvedimento del Garante, ha predisposto il presente Disciplinare che esplicita le eventuali forme di controllo messe in campo dall'Ente.

## Il controllo e gli obblighi di tutela

### a) Tutela e salvaguardia del patrimonio

La tutela del patrimonio dell'Istituto si inserisce in quel costante processo di "sicurezza informatica" che riflette la necessità di proteggere le informazioni e i dati interni da attacchi esterni di vario genere: sporadici e casuali come possono essere i virus, ma anche mirati e

preordinati per carpire o distruggere dati sensibili. I danneggiamenti ai sistemi informatici (intenzionali o meno) sono agevolati dalla negligenza dell'utente sprovveduto che, in assenza di controllo e di prescrizioni, potrebbe installare programmi nocivi al sistema, scaricare allegati sospetti disattivando la protezione, comunicare password, essere vittima di un attacco di social engineering, etc. Superfluo specificare gli ingenti danni che INVALSI sarebbe costretto a sopportare a causa di tali superficiali disattenzioni. Analizzare e prevenire tali rischi è più conveniente di riparare il danno già verificato.

La sicurezza informatica, una cui componente è sicuramente il controllo del traffico telematico, non può essere trascurata né sottovalutata da INVALSI. Inoltre, non è da sottovalutare il rischio di danni alla reputazione a cui è soggetto INVALSI dai cui indirizzi mail partono messaggi dal contenuto extra-lavorativo e di dubbio decoro, che, magari, vengono successivamente girati "a

**b) Responsabilità civile**

Il primo profilo di responsabilità a carico di INVALSI deriva dall'obbligo risarcitorio connesso alla commissione di un reato o di un fatto illecito da parte del dipendente. L'art. 2049 c.c. prevede che "*i padroni e i committenti sono responsabili per i danni arrecati dal fatto illecito dei loro domestici e commessi nell'esercizio delle incombenze a cui sono adibiti*". Alla stregua di questa norma, il terzo danneggiato può validamente chiedere il risarcimento del danno subito, non solo a colui che ha commesso direttamente il fatto (il dipendente), ma anche al datore di lavoro a prescindere da un'eventuale responsabilità penale di quest'ultimo.

**c) Responsabilità penale**

I comportamenti telematici illeciti del lavoratore possono essere penalmente rilevanti. In questo caso il coinvolgimento di INVALSI, ferma restando la responsabilità civile appena vista, può avere riflessi penali. Il nostro ordinamento prevede infatti la categoria dei cosiddetti "reati omissivi impropri", che si concretizzano nella violazione di un generico obbligo giuridico di impedire determinati eventi dannosi. La posizione di garanzia in capo al datore di lavoro, da cui deriva l'obbligo di controllo, deriva dal rapporto di lavoro stesso. Pertanto in caso di reato compiuto dal lavoratore, sarà perseguibile penalmente anche il datore di lavoro, a titolo di concorso nel reato, per non aver impedito l'azione adottando idonee misure di prevenzione e controllo.

A titolo esemplificativo si elencano alcuni reati commessi mediante Internet e reati commessi su Internet: ingiuria, diffamazione, istigazione a delinquere, apologia, rivelazione di segreti professionali o industriali, spamming, illecita duplicazione o distribuzione di programmi per

elaboratore, reati connessi alla pedopornografia, accesso abusivo ad un sistema informatico o telematico, detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici, reati contro l'integrità dei sistemi informatici e telematici, diffusione di programmi diretti a danneggiarli o interromperli, frode informatica, ecc.

Premesso tutto quanto sopra, la strumentazione tecnologica/informatica e quanto con essa creato è di proprietà di INVALSI, in quanto mezzo di lavoro. È di conseguenza vietato il suo utilizzo per fini ed interessi non strettamente coincidenti con quelli dell'Ente stesso. Quest'ultima potrebbe effettuare dei controlli sulle proprie apparecchiature tecnologiche al fine di preservare la sicurezza informatica dei dati personali in esse contenuti.
Inoltre, INVALSI promuove ogni opportuna misura, organizzativa e tecnologica volta a prevenire il rischio di utilizzi impropri e, comunque, a minimizzare l'uso di dati riferibili ai lavoratori e allo scopo ha adottato ogni possibile strumento tecnico, organizzativo e fisico, volto a prevenire trattamenti illeciti sui dati trattati con strumenti informatici. In particolare:

- Conformemente ai principi di pertinenza e non eccedenza, le verifiche sugli strumenti informatici saranno realizzati nel pieno rispetto dei diritti e delle libertà fondamentali delle persone autorizzate e del presente Disciplinare.
- 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:
    - ad esigenze tecniche o di sicurezza del tutto particolari;
    - all'indispensabilità del dato rispetto all'esercizio o alla difesa di un diritto in sede giudiziaria;
    - 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.

- In caso di anomalie INVALSI, per quanto possibile, privilegerà preliminari controlli anonimi e quindi riferiti a dati aggregati nell'ambito di intere strutture lavorative o di sue aree nelle quali si è verificata l'anomalia.

- 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 avviso al Responsabile dell'Area istituzionale interessata in cui è stato rilevato l'utilizzo anomalo degli strumenti dell'Istituto affinché lo stesso inviti le strutture da lui dipendenti ad attenersi scrupolosamente ai compiti assegnati e alle istruzioni impartite;
    - in caso di successive, perduranti anomalie, ovvero ravvisandone comunque la necessità, INVALSI si riserva di effettuare verifiche anche su base individuale, comunque finalizzate esclusivamente alla individuazione di eventuali condotte illecite.

In nessun caso verranno realizzate verifiche prolungate, costanti o indiscriminate, fatte salve le verifiche atte a tutelare gli interessi dell'Istituto.

**Responsabilità, provvedimenti disciplinari e sanzioni.**

Tutti i destinatari del presente Disciplinare sono tenuti a conformarsi alle indicazioni ivi presenti. Nessun soggetto operante all'interno di INVALSI potrà giustificare la propria condotta adducendo l'ignoranza del presente documento.
In caso di dubbi sulla condotta da tenere in concreto in relazione alle indicazioni su esposte, i destinatari sono tenuti a rivolgersi al superiore gerarchico per ricevere le opportune indicazioni.
In caso di dubbio in relazione al sistema sanzionatorio applicabile, il dipendente può chiedere delucidazioni all'ufficio del personale.
Il mancato rispetto o la violazione del Disciplinare, costituendo inadempimento contrattuale potrà comportare:

- per il personale dipendente oltre che l'adozione di provvedimenti di natura disciplinare previsti dal Contratto Collettivo Nazionale di Lavoro vigente, le azioni civili e penali stabilite dalle leggi vigenti;

- per i collaboratori esterni oltre che la risoluzione del contratto le azioni civili e penali stabilite dalle leggi vigenti, nonché eventuali azioni di rivalsa nei confronti dello stesso.

Se dalla violazione dovesse derivare un danno a INVALSI, quest'ultima si riserva la facoltà di richiedere al trasgressore il giusto risarcimento economico.

**Esercizio dei diritti dell'interessato.**

Il lavoratore interessato al trattamento dei dati può esercitare i propri diritti ai sensi degli articoli dal 15 al 22 del GDPR rivolgendosi al Titolare del trattamento.