CARTA INTESTATA

DISCIPLINARE RELATIVO ALL'UTILIZZO DEI DATI

Regole di condotta ed obblighi dei responsabili ed incaricati del trattamento dei dati personali, in relazione all'uso degli strumenti informatici, di Internet e della Posta Elettronica, redatto ai sensi del provvedimento del Garante della Privacy (Deliberazione n. 13 del 1/3/2007 - pubblicata in GU n. 58 del 10 marzo 2007) comprensivo di alcune note per la gestione dei dati cartacei ed adeguato al Regolamento Europeo 679/2016.

1. SEZIONE I

AMBITO GENERALE

1.1. Definizioni

Ente/organizzazione/Istituto: NOME ENTE"

Autorizzazione : il provvedimento adottato dal Garante con cui il titolare del trattamento (ente pubblico, impresa, libero professionista) viene autorizzato a trattare determinati dati "sensibili" o giudiziari, ovvero a trasferire dati personali all'estero.

Comunicazione: far conoscere dati personali a uno o più soggetti determinati (che non siano l'interessato, il sub-titolare o l'incaricato), in qualunque forma, anche attraverso la loro messa a disposizione o consultazione (vedi anche diffusione)

Consenso: la libera manifestazione di volontà dell'interessato con cui questi accetta espressamente un determinato trattamento dei suoi dati personali, del quale è stato preventivamente informato da chi ha un potere decisionale sul trattamento (vedi titolare).

D.Lgs. 196/2003: Decreto Legislativo 196 del 30 giugno 2003 e sue successive

modifiche ed integrazioni.

Dato personale: qualsiasi informazione che riguardi persone fisiche identificate o che possono essere identificate anche attraverso altre informazioni, ad esempio, attraverso un numero o un codice identificativo. Sono, ad esempio, dati personali: il nome e cognome o denominazione; l'indirizzo, il codice fiscale; ma anche

un’immagine, la registrazione della voce di una persona, la sua impronta digitale, i dati sanitari, i dati bancari, ecc.

Dato particolare (sensibile) : un dato personale che, per la sua natura, richiede particolari cautele: sono dati sensibili quelli che possono rivelare l’origine razziale ed etnica, le convinzioni religiose o di altra natura, le opinioni politiche, l’adesione a partiti, sindacati o associazioni, lo stato di salute e la vita sessuale delle persone.

Dato giudiziario: i dati personali che rivelano l’esistenza di determinati provvedimenti giudiziari soggetti ad iscrizione nel casellario giudiziale (quali, ad es., i provvedimenti penali di condanna definitivi, la liberazione condizionale, il divieto od obbligo di soggiorno, le misure alternative alla detenzione). Rientrano in questa categoria anche la qualità di imputato o di indagato.

Diffusione: divulgare dati personali al pubblico o, comunque, ad un numero indeterminato di soggetti (ad esempio, è diffusione la pubblicazione di dati personali su un quotidiano o su una pagina web).

Dipendente: personale dell’ ente/organizzazione/azienda assunto con qualsiasi tipo di forma

contrattuale, anche in stage o tirocinio.

GDPR General Data Protection Regulation - Regolamento Generale sulla Protezione dei Dati - UE 2016/679: è un Regolamento con il quale la Commissione europea intende

rafforzare e rendere più omogenea la protezione dei dati personali di cittadini dell’Unione Europea e dei residenti nell’Unione Europea, sia all’interno che all’esterno dei confini dell’Unione europea (UE). Il testo, pubblicato su Gazzetta Ufficiale Europea il 4 maggio 2016 ed entrato in vigore il 25 maggio dello stesso anno, inizierà ad avere efficacia il 25 maggio 2018.

Incaricato: ogni dipendente, come sopra identificato, ed ogni consulente esterno che, nell’ambito dell’attività assegnatagli, tratta dati (nell’accezione del capitolo seguente) riferiti all’Istituto. Il regolamento europeo non prevede espressamente la figura dell’incaricato, ma non ne esclude la nomina, facendo riferimento a persone autorizzate al trattamento dei dati sotto l’autorità diretta del titolare o del responsabile (art. 4). In sede europea, alla nostra DPA è stato concesso di poter utilizzare ancora i termini titolare, responsabile e incaricato; traducendo così, nella versione italiana del GDPR, la figura del “controller” (Art. 4.7) con “titolare del trattamento”; “processor” (Art. 4.8) con “responsabile del trattamento”; “third party” (Art. 4.10) con “terzo”, e di poter continuare ad utilizzare il termine “incaricato” per qualificare “le persone autorizzate al trattamento dei dati personali sotto l’autorità diretta del titolare o del responsabile”. Alla luce di ciò, si può identificare la figura di Incaricato in quella di Responsabile.

Informativa: le informazioni che il titolare del trattamento deve fornire ad ogni interessato, verbalmente o per iscritto quando i dati sono raccolti presso l’interessato stesso, oppure presso terzi. L’informativa deve precisare sinteticamente e in modo colloquiale quali sono gli scopi e le modalità del trattamento; se l’interessato è obbligato o no a fornire i dati; quali sono le conseguenze se i dati non vengono forniti; a chi possono essere comunicati o diffusi i dati; quali sono i diritti riconosciuti all’interessato; chi sono il titolare e l’eventuale responsabile del trattamento e dove sono raggiungibili (indirizzo, telefono, fax, ecc.).

Interessato: la persona fisica cui si riferiscono i dati personali.

Misure di sicurezza: sono tutti gli accorgimenti tecnici ed organizzativi, i dispositivi elettronici o i programmi informatici utilizzati per garantire che i dati non vadano distrutti o persi anche in modo accidentale, che solo le persone autorizzate possano avere accesso ai dati e che non siano effettuati trattamenti contrari alle norme di legge o diversi da quelli per cui i dati erano stati raccolti.

NDA: non-disclosure agreement, ovvero accordo di non divulgazione, è un negozio giuridico di natura sinallagmatica che designa informazioni confidenziali e con il quale le parti si impegnano a mantenerle segrete, pena la violazione dell'accordo stesso e il decorso di specifiche clausole penali in esso contenute.

Responsabile (del trattamento): la persona, la società, l'ente, l'associazione o l'organismo cui il

titolare affida, anche all'esterno, per la particolare esperienza o capacità, compiti di gestione e controllo del trattamento dei dati.

Titolare del trattamento: la persona fisica, l'impresa, l'ente, l'associazione, ecc. cui fa capo effettivamente il trattamento di dati personali e spetta assumere le decisioni fondamentali sugli scopi e sulle modalità del trattamento medesimo (comprese le misure di sicurezza). Nei casi in cui il trattamento sia svolto da una società o da una pubblica amministrazione per titolare va intesa l'entità nel suo complesso e non l'individuo o l'organo che l'amministra o la rappresenta (presidente, amministratore delegato, sindaco, ministro, direttore generale, ecc.).

Trattamento (di dati personali): un'operazione o un complesso di operazioni che hanno per oggetto dati personali.

1.2. Premessa

L'ambito lavorativo porta la nostra organizzazione a gestire una serie di "informazioni", proprie e di terzi, per poter erogare i servizi che le vengono istituzionalmente richiesti. Tali informazioni possono essere considerate, ai sensi del D. Lgs. 196/2003 e s.m.i., "dati personali" quando sono riferite a persone fisiche e, per la loro gestione (Trattamento), sia cartacea che digitale, è necessario che l'Istituto adotti una serie di misure minime ed idonee previste dalle norme. Altre informazioni, pur non essendo "dati personali" ai sensi di legge, sono in tutto e per tutto "informazioni riservate", ovvero informazioni tecniche, commerciali, contrattuali, di business o di altro genere per le quali l'organizzazione è chiamata a garantire la riservatezza, o per NDA, o per una più ampia tutela del patrimonio del titolare. Ai fini di questo disciplinare si specifica, pertanto, che con il termine "dati" deve intendersi l'insieme più ampio di informazioni di cui un dipendente o un collaboratore può venire a conoscenza e di cui deve garantire la riservatezza e la segretezza e non solo i "dati personali" intesi a norma di legge. Inoltre, nell'ambito della sua attività, il titolare spesso tratta "dati cartacei", ovvero informazioni su supporto cartaceo, e "dati digitali", ovvero informazioni che vengono memorizzate o semplicemente transitano attraverso apparecchiature digitali.

In linea generale, ogni dato, nell'accezione più ampia sopra descritta, di cui l'incaricato viene a conoscenza, nell'ambito della propria attività lavorativa, è da considerarsi riservato e non deve essere comunicato o diffuso a nessuno (anche una volta interrotto il rapporto lavorativo con l'organizzazione stessa o qualora parte delle informazioni siano di pubblico dominio) salvo specifica autorizzazione esplicita del titolare. Anche tra colleghi, oppure tra dipendenti e collaboratori esterni, è necessario

adottare la più ampia riservatezza nella comunicazione dei dati conosciuti, limitandosi solo a quei casi che si rendono necessari per espletare al meglio l’attività lavorativa richiesta.

La progressiva diffusione delle nuove tecnologie informatiche ed, in particolare, l'accesso alla rete internet dal computer aziendale, espone il Titolare a possibili rischi di un coinvolgimento di rilevanza sia civile, sia penale, sia amministrativa, creando problemi alla sicurezza e all'immagine dell'organizzazione stessa. Premesso che i comportamenti che normalmente si adottano nell'ambito di un rapporto di lavoro, tra i quali rientrano l'utilizzo delle risorse informatiche e telematiche, devono sempre ispirarsi al principio di diligenza e correttezza, il TITOLARE ha adottato il presente Disciplinare Interno, diretto ad evitare che condotte inconsapevoli possano innescare problemi o minacce alla sicurezza dei dati o delle attrezzature aziendali. Il presente Disciplinare Interno si applica ai Responsabili e Incaricati che si trovino ad operare con dati TITOLARE. Una gestione dei dati cartacei, un uso dei COMPUTER e di altre attrezzature elettroniche (di seguito DISPOSITIVI), nonché dei servizi internet e della posta elettronica difforme dalle regole contenute nel presente Disciplinare potrebbe esporre l'organizzazione ad aumentare la minaccia di accessi non autorizzati ai dati e/o al sistema informatico aziendale, furti o divulgazioni di informazioni riservate nonché furti o danneggiamenti del sistema informatico e/o malfunzionamenti in generale dell'intero sistema informatico. Le informazioni contenute nel presente Disciplinare vengono rilasciate ai sensi dell'art. 13 del Codice sulla Privacy e dell'art. 13 del Regolamento Europeo 679/2016, e costituiscono, quindi, parte integrante dell'informativa rilasciata ai Responsabili ed agli Incaricati.

1.3. Esclusione all'uso degli strumenti informatici

All'inizio del rapporto lavorativo o di consulenza, l'TITOLARE valuta la presenza dei presupposti per l'autorizzazione all'uso dei vari dispositivi aziendali, di internet e della posta elettronica da parte degli incaricati. Successivamente, e periodicamente, l'TITOLARE valuta la permanenza dei presupposti per l'utilizzo dei dispositivi aziendali, di internet e della posta elettronica. È fatto esplicito divieto ai soggetti non autorizzati di accedere agli strumenti informatici aziendali. I casi di esclusione possono riguardare: 1. L'utilizzo del COMPUTER o di altri DISPOSITIVI. 2. L'utilizzo della posta elettronica. 3. L'accesso a internet. Le eventuali esclusioni sono strettamente connesse al principio della natura aziendale e lavorativa degli strumenti informatici, nonché al principio di necessità di cui al Codice Privacy e GDPR. Più specificatamente, hanno diritto all'utilizzo degli strumenti e ai relativi accessi solo i responsabili che, per funzioni lavorative, ne abbiano un effettivo e concreto bisogno. I casi in cui le esclusioni dovranno risultare operative in forza di tali motivazioni verranno comunicati individualmente e potranno riguardare sia tutti i casi sopra descritti, sia solo uno o due degli stessi. Si informa che tali esclusioni sono divenute necessarie alla luce del Provvedimento del Garante 1° marzo 2007, che indica di ridurre a titolo cautelativo e preventivo l'utilizzo degli strumenti informatici in considerazione dei pericoli e delle minacce indicate in questo documento.

1.4. Titolarità dei dispositivi e dei dati

L'organizzazione è esclusiva titolare e proprietaria dei dispositivi messi a disposizione dei responsabili, ai soli fini dell'attività lavorativa. L'TITOLARE è l'unico esclusivo titolare e proprietario di tutte le informazioni, le registrazioni ed i dati contenuti e/o trattati mediante i propri dispositivi digitali o archiviati in modo cartaceo nei propri locali. Il Responsabile non può presumere o ritenere che le informazioni, le registrazioni ed i dati da lui trattati o memorizzati nei dispositivi aziendali (inclusi i messaggi di posta elettronica e/o chat inviati o ricevuti, i file di immagini, i files di filmati o altre tipologie di files) siano privati o personali, né può presumere che dati cartacei in suo possesso possano essere da lui copiati, comunicati o diffusi senza l'autorizzazione dell'organizzazione.

1.5. Finalità nell’utilizzo dei dispositivi

I dispositivi assegnati sono uno strumento lavorativo nelle disponibilità del Responsabile esclusivamente per un fine di carattere lavorativo. I dispositivi, quindi, non devono essere utilizzati per finalità private e diverse da quelle istituzionali, se non eccezionalmente e nei limiti evidenziati dal presente Disciplinare.

Qualsiasi eventuale tolleranza da parte di questo TITOLARE, apparente o effettiva, non potrà, comunque, legittimare comportamenti contrari alle istruzioni contenute nel presente Disciplinare.

1.6. Restituzione dei dispositivi

A seguito di una cessazione del rapporto lavorativo o di consulenza del Responsabile con l'organizzazione o, comunque, al venir meno, ad insindacabile giudizio dell'TITOLARE, della permanenza dei presupposti per l'utilizzo dei dispositivi aziendali, i responsabili hanno i seguenti obblighi: 1. Procedere immediatamente alla restituzione dei dispositivi in uso. 2. Divieto assoluto di formattare o alterare o manomettere o distruggere i dispositivi assegnati o

rendere inintelligibili i dati in essi contenuti, tramite qualsiasi processo.

1.7. Restituzione dei dati cartacei

A seguito di una cessazione del rapporto lavorativo o di consulenza del responsabile con l'organizzazione o, comunque, al venir meno, ad insindacabile giudizio dell'TITOLARE, della permanenza dei presupposti per l'utilizzo di dati cartacei aziendali, gli incaricati hanno i seguenti obblighi: 1. Procedere immediatamente alla restituzione dei dati cartacei in loro possesso. 2. Divieto assoluto di alterare o manomettere o distruggere i dati cartacei assegnati o renderli

inintelligibili, tramite qualsiasi processo.

2. SEZIONE II

PASSWORD

2.1. Le Password

Le password possono essere un metodo di autenticazione assegnato dall'organizzazione per garantire l'accesso protetto ad uno strumento hardware, oppure ad un applicativo software. La prima caratteristica di una password è la segretezza, e cioè il fatto che non venga svelata ad altri soggetti. La divulgazione delle proprie password o la trascuratezza nella loro conservazione può causare gravi danni al proprio lavoro, a quello dei colleghi e dell'TITOLARE nel suo complesso. Nel tempo, anche la password più sicura perde la sua segretezza. Per questo motivo è buona norma cambiarle con una certa frequenza. L'TITOLARE ha implementato alcuni meccanismi che permettono di aiutare e supportare gli Incaricati in una corretta gestione delle password, in particolare, per quanto riguarda le password di accesso ad ogni dispositivo utilizzato (sia fisico che on line), in particolare nel settore amministrativo. Password che vengono aggiornate periodicamente secondo il livello di sicurezza richiesto dall'TITOLARE stesso e, comunque, in linea con quanto richiesto dalla normativa privacy. Altra buona norma è quella di non memorizzare la password su supporti facilmente intercettabili da altre persone. Il miglior luogo in cui conservare una password è la propria memoria. Le password che non vengono utilizzate da parte dei responsabili per un periodo superiore ai sei mesi, verranno disattivate dall'TITOLARE. In qualsiasi momento, l'organizzazione si riserva il diritto di revocare al responsabile il permesso di accedere ad un sistema hardware o software a cui era precedentemente autorizzato, rimuovendo user id o modificando/cancellando la password ad esso associata.

2.2. Regole per la corretta gestione delle password

Il responsabile, da parte sua, per una corretta e sicura gestione delle proprie password, deve rispettare le regole seguenti: 1. Le password sono assolutamente personali e non vanno mai comunicate ad altri. 2. Occorre cambiare immediatamente una password, non appena si abbia alcun dubbio che sia

diventata poco “sicura”. 3. Le password devono essere lunghe almeno 8 caratteri e devono contenere anche lettere maiuscole,

caratteri speciali1 e numeri. 4. Le password non devono essere memorizzate su alcun tipo di supporto, quali, ad esempio, Post-It

(sul monitor o sotto la tastiera) o agende (cartacee, posta elettronica, telefono cellulare). 5. Le password devono essere sostituite almeno nei tempi indicati dalla normativa, a prescindere

dall’esistenza di un sistema automatico di richiesta di aggiornamento password. 6. Evitare di digitare la propria password in presenza di altri soggetti che possano vedere la tastiera, anche se collaboratori o dipendenti dell’TITOLARE. In alcuni casi, sono implementati meccanismi che consentono al responsabile un numero limitato di tentativi errati di inserimento della password, oltre ai quali il tentativo di accesso viene considerato un attacco al sistema e l’account viene bloccato per alcuni minuti. In caso di necessità, contattare il Titolare.

2.3. Divieto di uso

Al fine di una corretta gestione delle password, l’organizzazione stabilisce il divieto di utilizzare come propria password: 1. Nome, cognome e loro parti. 2. Lo username assegnato. 3. Un indirizzo di posta elettronica (e-mail). 4. Parole comuni (in Inglese e in Italiano). 5. Date, mesi dell’anno e giorni della settimana, anche in lingua straniera. 6. Parole banali e/o di facile intuizione, ad es. pippo, security e palindromi (simmetria: radar). 7. Ripetizioni di sequenze di caratteri (es. abcabcabc). 8. Una password già impiegata in precedenza.

2.3.1. Alcuni esempi di password non ammesse

La password ideale deve essere complessa, senza alcun riferimento, ma facile da ricordare. Una possibile tecnica è usare sequenze di caratteri prive di senso evidente, ma con singoli caratteri che formano una frase facile da memorizzare (es.: “NIMzz5DICmm!”, Nel Mezzo Del Cammin, più il carattere 5 e il punto esclamativo). Decifrare una parola come questa può richiedere giorni, una come “radar” meno di dieci secondi. Alcuni esempi di password assolutamente da evitare: 1. Se Username = “mariorossi”, password = “mario”, o ancora peggio, password = “mariorossi”. 2. Il nome della moglie/marito, fidanzato/a, figli, ecc. anche a rovescio! 3. La propria data di nascita, quella del coniuge, ecc. 4. Targa della propria auto. 5. Numero di telefono proprio, del coniuge, ecc. 6. Parole comuni tipo “Kilimangiaro”, “Password”, “Qwerty”, “12345678” (troppo facili). 7. Qualsiasi parola del vocabolario (di qualsiasi lingua diffusa, come inglese, italiano, ecc.).

2.4. La password nei sistemi

Ogni Responsabile può variare la propria password di accesso a qualsiasi sistema aziendale in modo autonomo, qualora il sistema in questione metta a disposizione degli Utenti una funzionalità di questo tipo (Change password), oppure facendone richiesta al Titolare. La password può essere sostituita dal Titolare, anche qualora l’Utente l’abbia dimenticata.

2.5. Audit delle password

Nell'ambito delle attività riguardanti la tutela della sicurezza della infrastruttura tecnologica, l'TITOLARE potrebbe effettuare analisi periodiche sulle password degli Incaricati al fine di verificarne la solidità, le policy di gestione e la durata, informandone preventivamente gli Responsabili stessi.

1 Per caratteri speciali si intendono, per esempio, i seguenti: { } [ ], . < > ; : ! " £ $ % & / ( ) = ? ^ \ | ' * - + _.

Nel caso in cui l'audit abbia, tra gli esiti possibili, la decodifica della password, questa viene bloccata e richiesto al Responsabile di cambiarla.

3. SEZIONE III

OPERAZIONI A PROTEZIONE DELLA POSTAZIONE DI LAVORO

In questa sezione vengono trattate le operazioni a carico del Responsabile e il quadro di riferimento generale per l'esecuzione di operazioni a protezione della propria postazione di lavoro, nel rispetto della sicurezza e dell'integrità del patrimonio aziendale.

3.1. Login e Logout

Il "Login" è l'operazione con la quale il Responsabile si connette al sistema informativo aziendale o ad una parte di esso, dichiarando il proprio Username e Password (ossia l'Account), aprendo una sessione di lavoro. In molti casi è necessario effettuare più login, tanti quanti sono gli ambienti di lavoro (ad es. applicativi web, Intranet), ognuno dei quali richiede uno username e una password. In questi casi, sebbene sia preferibile che ogni utente abbia un suo specifico user name e password, l'TITOLARE potrà assegnare un univoco user name e password per gruppi di responsabili per l'accesso alla macchina fisica, mentre rimarranno separati ed univoci per l'accesso agli applicativi che contengono dati. Il "Logout" è l'operazione con cui viene chiusa la sessione di lavoro. Al termine della giornata lavorativa, tutte le applicazioni devono essere chiuse secondo le regole previste dall'applicazione stessa. La non corretta chiusura può provocare una perdita di dati o l'accesso agli stessi da parte di persone non autorizzate. Il "blocco del computer" è l'operazione con cui viene impedito l'accesso alla sessione di lavoro (tastiera e schermo disattivati) senza chiuderla.

3.2. Obblighi

L'utilizzo dei dispositivi fisici e la gestione dei dati ivi contenuti devono svolgersi nel rispetto della sicurezza e dell'integrità del patrimonio dati aziendale. Il responsabile deve quindi eseguire le operazioni seguenti: 1. Se si allontana dalla propria postazione, dovrà mettere in protezione il suo dispositivo affinché

persone non autorizzate non abbiano accesso ai dati protetti. 2. Bloccare il suo dispositivo prima delle pause e, in generale, ogni qualvolta abbia bisogno di

allontanarsi dalla propria postazione; 3. Chiudere la sessione (Logout) a fine giornata; 4. Spegnere il PC dopo il Logout; 5. Controllare sempre che non vi siano persone non autorizzate alle sue spalle che possano prendere

visione delle schermate del suo dispositivo.

4 SEZIONE IV USO DEL PERSONAL COMPUTER DELL'ENTE

4.1. Modalità d'uso del COMPUTER aziendale

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

I file creati, elaborati o modificati sul computer assegnato devono essere poi sempre salvati a fine giornata sul sistema di repository documentale centralizzato. L'TITOLARE non effettua il backup dei dati memorizzati in locale.

4.2. Corretto utilizzo del COMPUTER aziendale

Il computer consegnato al responsabile è uno strumento di lavoro e contiene tutti i software necessari a svolgere le attività affidate. Ogni utilizzo non inerente all'attività lavorativa può contribuire ad innescare disservizi, rallentamenti del sistema, costi di manutenzione e, soprattutto, minacce alla sicurezza. L'accesso all'elaboratore è protetto da password che deve essere custodita dall'responsabile con la massima diligenza e non divulgata. Il computer che viene consegnato contiene tutti i software necessari a svolgere le attività affidate dall'organizzazione. Per necessità aziendali, gli amministratori di sistema utilizzando la propria login con privilegi di amministratore e la password dell'amministratore, potranno accedere, con le regole indicate nel presente documento, sia alle memorie di massa locali di rete (repository e backup) che ai server aziendali nonché, previa comunicazione al dipendente, accedere al computer, anche in remoto. In particolare il Responsabile deve adottare le seguenti misure: 1. Utilizzare solo ed esclusivamente le aree di memoria della rete dell'TITOLARE ed ivi creare e registrare

file e software o archivi dati, senza pertanto creare altri file fuori dalle unità di rete. 2. Spegnere il computer, o curarsi di effettuare il Logout, ogni sera prima di lasciare gli uffici o in caso di assenze prolungate, poiché lasciare un elaboratore incustodito connesso alla rete può essere causa di utilizzo da parte di terzi, senza che vi sia la possibilità di provarne in seguito l'indebito uso. 3. Mantenere sul computer esclusivamente i dispositivi di memorizzazione, comunicazione o altro

(come ad esempio masterizzatori), disposti dall'organizzazione. 4. Non dare accesso al proprio computer ad altri utenti, a meno che siano responsabili con cui condividono l'utilizzo dello stesso Pc o a meno di necessità stringenti e sotto il proprio costante controllo.

4.3. Divieti Espressi sull'utilizzo del COMPUTER

Al responsabile è vietato: 1. La gestione, la memorizzazione (anche temporanea) o il trattamento di file, documenti e/o informazioni personali del responsabile o comunque non afferenti alle attività lavorative nella rete, nel disco fisso o in altre memorie di massa aziendali e negli strumenti informatici aziendali in genere. 2. Modificare le configurazioni già impostate sul personal computer. 3. Utilizzare programmi e/o sistemi di criptazione senza la preventiva autorizzazione scritta

dell'TITOLARE. 4. Installare alcun software di cui l'TITOLARE non possieda la licenza, né installare alcuna versione diversa, anche più recente, rispetto alle applicazioni o al sistema operativo presenti sul personal computer consegnato, senza l'espressa autorizzazione dell'organizzazione. È, peraltro, vietato fare copia del software installato al fine di farne un uso personale. 5. Caricare sul disco fisso del computer o nel server documenti, giochi, file musicali o audiovisivi o

immagine diversi da quelli necessari allo svolgimento delle mansioni affidate. 6. Aggiungere o collegare dispositivi hardware (ad esempio hard disk, driver, PCMCIA, ecc.) o periferiche (telecamere, macchine fotografiche, smartphone, chiavi USB ecc.) diversi da quelli consegnati, senza l'autorizzazione espressa dell'organizzazione. 7. Creare o diffondere, intenzionalmente o per negligenza, programmi idonei a danneggiare il sistema

informatico dell’organizzazione, quali per esempio virus, trojan horses e malware in genere. 8. Accedere, rivelare o utilizzare informazioni non autorizzate o comunque non necessarie per le

mansioni svolte. 9. Effettuare in proprio attività manutentive. 10. Permettere attività manutentive da parte dei soggetti non espressamente autorizzati

dell’organizzazione.

4.4. ANTIVIRUS

I virus (o, per essere precisi, il malware, il software malevolo) possono essere trasmessi tramite scambio di file via internet, via mail, scambio di supporti removibili, filesharing, chat, via mail ... L'TITOLARE impone su tutte le postazioni di lavoro l'utilizzo di un sistema antivirus correttamente installato, attivato continuamente e aggiornato automaticamente con frequenza almeno quotidiana. Il responsabile, da parte sua, deve impegnarsi a controllare il corretto funzionamento e aggiornamento del sistema antivirus installato sul proprio computer e, in particolare, deve rispettare le regole seguenti: 1. Comunicare all'TITOLARE ogni anomalia o malfunzionamento del sistema antivirus. 2. Comunicare all'TITOLARE eventuali segnalazioni di presenza di virus o file sospetti.

Inoltre, al responsabile: 1. È vietato accedere alla rete aziendale senza servizio antivirus attivo e aggiornato sulla propria

postazione. 2. È vietato ostacolare l'azione dell'antivirus aziendale. 3. È vietato disattivare l'antivirus senza l'autorizzazione espressa dell'TITOLARE, anche e soprattutto nel

caso sia richiesto per l'installazione di software sul computer. 4. È vietato aprire allegati di mail provenienti da mittenti sconosciuti o di dubbia provenienza o allegati di mail di persone conosciute ma con testi inspiegabili o in qualche modo strani. Contattare i sistemi informativi prima di procedere a qualsiasi attività potenzialmente in conflitto con quanto sopra.

5 SEZIONE V

INTERNET

5.1. Internet è uno strumento di lavoro

La connessione alla rete internet dal dispositivo avuto in dotazione è ammessa esclusivamente per motivi attinenti allo svolgimento dell'attività lavorativa. L'utilizzo per scopi personali è permesso con moderazione e con gli accorgimenti di cui al presente documento. In particolare, si vieta l'utilizzo dei social network, se non espressamente autorizzati.

5.2. Misure preventive per ridurre navigazioni illecite

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

5.3. Divieti Espressi concernenti Internet

– È vietata la navigazione nei siti che possono rivelare le opinioni politiche religiose, sindacali e di salute del Responsabile poiché potenzialmente idonea a rivelare dati sensibili ai sensi del Codice Privacy. – 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 vietato al Responsabile lo scarico (download) di software (anche gratuito) prelevato da siti

Internet; – È tassativamente vietata l'effettuazione di ogni genere di transazione finanziaria, ivi comprese le operazioni di remote banking, acquisti on-line e simili, salvo i casi direttamente autorizzati dal Titolare e con il rispetto delle normali procedure di acquisto. – È vietata ogni forma di registrazione a

siti i cui contenuti non siano legati all'attività lavorativa. – È vietata la partecipazione a forum non professionali, l'utilizzo di chat line, di bacheche elettroniche o partecipare a gruppi di discussione o lasciare commenti ad articoli o iscriversi a mailing list spendendo il marchio o la denominazione dell'organizzazione, salvo specifica autorizzazione dell'organizzazione stessa.

– 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 Responsabile di promuovere utile o guadagno personale attraverso l'uso di Internet o

della posta elettronica aziendale. – È vietato accedere dall'esterno alla rete interna dell'organizzazione, salvo con le specifiche

procedure previste dall'TITOLARE stesso. – È vietato, infine, creare siti web personali sui sistemi dell'organizzazione, nonché acquistare beni o servizi su Internet, a meno che l'articolo acquistato non sia stato approvato a titolo di spesa professionale. 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 del Responsabile inadempiente.

5.4. Divieti di Sabotaggio

È vietato accedere ad alcuni siti internet mediante azioni inibenti dei filtri, sabotando o comunque superando o tentando di superare o disabilitando i sistemi adottati dall'TITOLARE per bloccare accessi non conformi all'attività lavorativa. In ogni caso è vietato utilizzare siti o altri strumenti che realizzino tale fine.

5.5. Diritto d'autore

È vietato utilizzare l'accesso ad internet, in violazione delle norme in vigore nell'ordinamento giuridico italiano a tutela del diritto d'autore (es. legge 22 aprile 1941, n. 633 e successive modificazioni, D. Lgs. 6 maggio 1999, n. 169 e legge 18 agosto 2000, n. 248). In particolare, è vietato il download di materiale soggetto a copyright (testi, immagini, musica, filmati, file in genere, ...) se non espressamente autorizzato dall'organizzazione.

6 SEZIONE VI POSTA ELETTRONICA

6.1. La Posta Elettronica è uno strumento di lavoro

L'utilizzo della posta elettronica aziendale è connesso allo svolgimento dell'attività lavorativa. L'uso per motivi personali deve essere moderato ed è tollerato esclusivamente ai sensi dell'articolo seguente. Gli Responsabili possono avere in utilizzo indirizzi nominativi di posta elettronica. Le caselle e-mail possono meglio essere assegnate con natura impersonale (tipo info, amministrazione, fornitori, direttore, collaboratore, consulenza, ...) proprio per evitare ulteriormente che il destinatario delle mail possa considerare l'indirizzo assegnato al dipendente "privato", ai sensi dei suggerimenti del Garante a tal proposito. I Responsabili assegnatari delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse.

6.2. Misure Preventive per ridurre utilizzi illeciti della Posta Elettronica

L'organizzazione è consapevole della possibilità di un limitato utilizzo personale della posta elettronica da parte degli Responsabili e allo scopo prevede le seguenti misure: 1. In caso di ricezione sulla e-mail aziendale di posta personale, si avverte di cancellare

immediatamente ogni messaggio, al fine di evitare ogni eventuale e possibile back up dei dati. 2. Avvisare l'organizzazione quando alla propria posta personale siano allegati files eseguibili e/o di

natura incomprensibile o non conosciuta.

6.3. Divieti Espressi

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

autorizzazione scritta dell'organizzazione, nonché utilizzare il dominio dell'organizzazione per scopi personali. 2. È vietato scrivere e generare messaggi di posta elettronica utilizzando l'indirizzo aziendale, diretti a

destinatari esterni dell'organizzazione, senza utilizzare il seguente disclaimer: «Il presente messaggio e gli eventuali suoi allegati sono di natura aziendale, prevalentemente confidenziale e sono visionabili solo dal destinatario di posta elettronica. La risposta o l'eventuale invio spontaneo da parte vostra di e-mail al nostro indirizzo potrebbero non assicurare la confidenzialità potendo essere viste da altri soggetti appartenenti all'organizzazione oltre al sottoscritto, per finalità di sicurezza informatica, amministrative e allo scopo del continuo svolgimento dell'attività aziendale. Qualora questo messaggio vi fosse pervenuto per errore, vi preghiamo di cancellarlo dal vostro sistema e vi chiediamo di volercene dare cortesemente comunicazione al mittente". 3. È vietato creare, archiviare o spedire, anche solo all'interno della rete aziendale, messaggi pubblicitari o promozionali o comunque allegati (filmati, immagini, musica o altro) non connessi con lo svolgimento della propria attività lavorativa, nonché partecipare a richieste, petizioni, mailing di massa di qualunque contenuto, "catene di Sant'Antonio" o in genere a pubblici dibattiti utilizzando l'indirizzo aziendale. 4. È vietato trasmettere messaggi a gruppi numerosi di persone (es. a tutto un ufficio o ad un'intera

divisione) senza l'autorizzazione necessaria. 5. È vietato sollecitare donazioni di beneficenza, propaganda elettorale o altre voci non legate al

lavoro. 6. È vietato utilizzare il servizio di posta elettronica per trasmettere a soggetti esterni dell'organizzazione informazioni riservate o comunque documenti aziendali, se non nel caso in cui ciò sia necessario in ragione delle mansioni svolte. 7. È vietato utilizzare la posta elettronica per messaggi con allegati di grandi dimensioni.

Nella definizione delle regole d'uso del servizio di posta elettronica e delle modalità di controllo, il MIUR ritiene di grande importanza salvaguardare la libertà di espressione e di pensiero e la garanzia della privacy dell'individuo. Questa Politica rispetta quindi i principi basilari esposti, nel contesto delle obbligazioni legali e delle politiche di sicurezza dell'Amministrazione. L'Amministrazione, anche sulla base delle direttive del governo tese a promuovere la crescita delle comunicazioni in formato digitale e l'abbattimento di quelle cartacee, considera la posta elettronica uno strumento fondamentale, che viene messo a disposizione di tutti coloro che ne abbiano diritto. La presente politica vale anche come informativa sulle finalità e modalità del trattamento dei dati personali, ricavabili dalle attività di controllo tecnico svolte sul servizio di posta elettronica, ai sensi dell'art. 13 della legge 196/2003.

Le condizioni di utilizzo della casella di posta elettronica xy.zw@istruzione.it, fissate dal MIUR, sono le seguenti:

a. Finalità del servizio di posta elettronica. Il MIUR incoraggia l'uso della posta elettronica per scambiare informazioni, migliorare le comunicazioni, scambiare idee e per rendere più efficaci ed efficienti i processi di lavoro a supporto della missione istituzionale dell'Amministrazione. b. Proprietà del MIUR: il servizio di posta elettronica del MIUR, erogato per il tramite dei Fornitori dei servizi in outsourcing, è proprietà del MIUR, pertanto ogni casella di posta elettronica associata al Ministero (nel dominio istruzione.it) o a suoi uffici o assegnata a individui o funzioni del Ministero, sono di proprietà del MIUR. c. Oneri a carico dell'Utente. Il servizio di posta elettronica è attivato, qualora ne abbia diritto, su richiesta dell'Utente ed è gratuito; resta a carico dell'Utente l'onere di dotarsi della strumentazione tecnica

necessaria per accedere al Servizio, ivi compresa l'eventuale spesa connessa al traffico telefonico sostenuto. Per usufruire del servizio è necessario registrarsi. Con la registrazione, l'Utente dichiara di aver letto e accettato tutti i termini e le condizioni di utilizzo del Servizio indicate nel documento. In mancanza dell'accettazione, il servizio non potrà essere attivato. Il MIUR fornisce all'Utente che richieda l'attivazione del servizio un codice Utente ed una password modificabile. L'accesso al Servizio è consentito solo mediante tali identificativi. d. Limitazioni di Responsabilità per il Ministero. Il MIUR non può essere ritenuto responsabile per qualsiasi danno, diretto o indiretto, arrecato all'Utente ovvero a terzi e derivante: – dall'eventuale interruzione del Servizio – dall'eventuale smarrimento di messaggi diffusi per mezzo del Servizio – da messaggi inviati/ricevuti o da transazioni eseguite tramite il Servizio – da accesso non autorizzato ovvero da alterazione di trasmissioni o dati dell'Utente. e. Restrizioni all'uso del servizio. Gli utenti del servizio di posta elettronica sono tenuti ad usarlo in modo responsabile, cioè, rispettando le leggi, la presente e altre politiche e procedure del

Ministero e secondo normali standard di cortesia, correttezza, buona fede e diligenza professionale. L'accesso ai servizi di posta elettronica dall'Amministrazione può essere totalmente o parzialmente limitato dall'Amministrazione stessa, senza necessità di assenso da parte dell'utente e anche senza preavviso: quando richiesto dalla legge e in conformità ad essa in caso di comprovati motivi che facciano ritenere la violazione della presente politica o delle disposizioni di legge vigenti al venir meno delle condizioni in base alle quali si ha facoltà di utilizzare il servizio (ad es. cessazione per qualsiasi motivo del rapporto di lavoro con l'Amministrazione) in casi eccezionali, quando richiesto per esigenze operative critiche e improcrastinabili. f. L'accesso ai servizi di posta elettronica può essere disattivato dall'Amministrazione in caso di cessazione del rapporto di lavoro o di non utilizzo della stessa per un periodo superiore ai 9 mesi, senza necessità di assenso da parte dell'utente. Non è prevista alcuna forma di indennizzo per il venir meno del servizio. g. Assenso e Conformità. Il MIUR è tenuto in generale ad ottenere l'assenso del titolare della casella di posta elettronica prima di ogni ispezione dei messaggi o accesso alle registrazioni o ai messaggi di posta elettronica, fatta eccezione per quanto disposto al punto g). D'altro canto, ci si attende che il personale del Ministero soddisfi le richieste dell'Amministrazione riguardanti la fornitura di copie delle registrazioni di posta elettronica in suo possesso che riguardino le attività lavorative del Ministero o richieste per soddisfare obblighi di legge, indipendentemente dal fatto che tali registrazioni risiedano o meno su computer di proprietà dell'Amministrazione. Il mancato rispetto di tali richieste può portare all'applicazione delle condizioni di cui la punto g). h. Limitazioni all'accesso senza assenso. Il MIUR non ispeziona e non accede ai messaggi di posta elettronica dell'utente senza la sua autorizzazione. D'altro canto, il Ministero potrà permettere l'ispezione, il monitoraggio o l'accesso alla posta elettronica degli utenti, anche senza l'assenso del titolare, solamente nei seguenti casi:

• su richiesta scritta dell'autorità giudiziaria nei casi previsti dalla normativa vigente

• previo preavviso all'utente, per gravi e comprovati motivi2, che facciano credere che siano state violate le disposizioni di legge vigenti o le politiche del MIUR in materia di sicurezza

• per atti dovuti3;

• in situazioni critiche e di emergenza4. i. Registro elettronico. L'Amministrazione registra e conserva, in forma anonima, i dati delle caselle di posta elettronica messe a disposizione dei propri utenti, tramite scrittura in appositi file di log, delle seguenti informazioni minime per ogni messaggio:

o mittente o destinatario/i o giorno ed ora dell'invio o esito dell'invio. o I file di registro sono conservati per un periodo di due anni.

AVVERTENZE Gli utenti del servizio di posta elettronica sono avvisati del fatto che: 1. La natura stessa della posta elettronica la rende meno sicura di quanto si possa immaginare. Ad esempio, i messaggi di posta elettronica spediti ad una persona possono essere facilmente inoltrati ad altri destinatari. Il Ministero non può proteggere gli utenti da fatti come quelli descritti che esulano dalle proprie possibilità e compiti. Gli utenti pertanto devono esercitare la massima cautela nell'uso della posta elettronica per comunicare informazioni riservate o dati sensibili. 2. I messaggi di posta elettronica, creati e conservati sia su apparati elettronici forniti

2

Grave e comprovato motivo: evidenza oggettiva, non basata quindi su semplici sospetti o illazioni, che dimostra l'avvenuta violazione di disposizioni di leggi vigenti o delle politiche di sicurezza dell'Amministrazione.

3

Atti dovuti: circostanze in base alle quali la mancanza di adeguate azioni può comportare danni significativi a cose o persone, perdita di informazioni di rilievo per l'Amministrazione o danni economici e di immagine per l'Amministrazione e per le persone che ne fanno parte.

4

Situazioni critiche o di emergenza: circostanze in cui la tempestività d'azione è di fondamentale importanza al fine di evitare danni significativi a cose o persone, perdita di informazioni di rilievo per l'Amministrazione o danni economici e di immagine per l'Amministrazione e per le persone che ne fanno parte o l'interruzione dei servizi informatici e la continuità operativa dei processi

dall'Amministrazione che su altri sistemi, possono costituire registrazioni di attività svolte dall'utente nell'espletamento delle sue attività lavorative. È possibile quindi che venga richiesto di accedere ai contenuti dei messaggi per un eventuale utilizzo nell'ambito di contenziosi che coinvolgano l'Amministrazione. Il MIUR non darà corso automaticamente a tutte le richieste di accesso, ma le valuterà in relazione a precisi obblighi di legge quali la privacy ed altre normative applicabili. Gli utenti devono però tener presente che, per quanto detto, in nessun caso l'Amministrazione può garantire che non saranno accedute informazioni personali degli utenti presenti in messaggi di posta elettronica residenti sui sistemi dell'Istruzione. 3. Il MIUR, in generale, non può e non intende porsi come valutatore dei contenuti dei messaggi di email scambiati, né può proteggere gli utenti dalla ricezione di messaggi che possano essere considerati offensivi. Gli utenti sono comunque fortemente incoraggiati a usare nella posta elettronica le stesse regole di cortesia che adopererebbero in altre forme di comunicazione. 4. Non c'è garanzia, a meno di utilizzare sistemi di posta certificata, che i messaggi ricevuti provengano effettivamente dal mittente previsto, perché è piuttosto semplice per i mittenti mascherare la propria identità, anche se ciò costituisce, tra le altre cose, una violazione della presente politica. Inoltre i messaggi di posta che arrivano come "inoltro" di precedenti messaggi, potrebbero essere stati modificati rispetto all'originale. Pertanto, in caso di dubbi, chi riceve un messaggio di posta elettronica dovrebbe verificare con il mittente l'autenticità delle informazioni ricevute.

USO CONSENTITO

L'uso del servizio di posta elettronica del MIUR è soggetto alle seguenti condizioni:

a. Proibizioni. È fatto divieto a tutti gli utenti di utilizzare il servizio di posta elettronica per inviare messaggi dannosi, di tipo offensivo o sconveniente, come ad esempio, a titolo non esaustivo, messaggi che riportino contenuti o commenti oltraggiosi su argomenti sessuali, razziali, religiosi, politici, ecc. e comunque ogni altra tipologia di messaggio che possa arrecare danno alla reputazione del MIUR. È inoltre vietato l'uso del servizio di posta elettronica a scopi commerciali o di profitto personale e per attività illegali e la fornitura (gratuita o a pagamento) a persone fisiche o giuridiche di qualsiasi lista o elenco degli Utenti del Servizio. È proibito fornire le proprie credenziali di accesso a sistemi o procedure, così come rispondere a messaggi email che facciano richiesta di questo tipo di informazioni. Chiunque riceva comunicazioni della natura sopra indicata dovrà segnalarlo alla Direzione Generale per i contratti, gli acquisti e per i sistemi informativi e la statistica utilizzando i servizi di assistenza online accessibili attraverso il sito Internet del MIUR. b. Uso Personale. È consentito l'utilizzo ragionevole del proprio account nel dominio "istruzione.it" a fini privati e personali, purché, in aggiunta a quanto indicato nei punti precedenti, tale utilizzo non:

• sia causa, diretta o indiretta di disservizi dei sistemi elaborativi e dei servizi di posta elettronica dell'Amministrazione;

• sia causa di oneri aggiuntivi per l'Amministrazione; o

• interferisca con le attività lavorative dell'utente o con altri obblighi dello stesso verso l'Amministrazione. L'utente è edotto del fatto che l'Amministrazione considererà, ai fini di eventuali ispezioni, tutti i messaggi di posta elettronica da lui gestiti come strettamente afferenti all'uso del servizio per scopi di lavoro. L'Amministrazione presuppone quindi che l'utente decida di utilizzare la posta elettronica per scopi personali avendone preliminarmente e attentamente valutato l'opportunità. Si ricorda comunque che per gli usi personali è possibile dotarsi di una casella di posta elettronica alternativa,

ottenibile gratuitamente presso molti fornitori esterni, e liberamente consultabile via internet.

SICUREZZA E RISERVATEZZA

Oltre a quanto indicato ai paragrafi precedenti, gli utenti devono tener presente che, nell'assolvimento dei propri compiti, il personale che gestisce i sistemi di elaborazione e le reti di telecomunicazione può avere, saltuariamente, la necessità di analizzare i dati transazionali dei messaggi di posta per garantire il corretto funzionamento del servizio e in queste occasioni è possibile che avvengano inavvertitamente accessi al contenuto stesso dei messaggi. Tale personale è tenuto comunque al rispetto di stretti vincoli di riservatezza qualora di verificassero i casi citati. Il Ministero della Pubblica Istruzione si pone come obiettivo fondamentale la fornitura di servizi di posta elettronica sicuri ed affidabili avvalendosi di fornitori altamente qualificati. Va comunque ricordato, come già detto in precedenza, che la sicurezza e riservatezza della posta elettronica non possono essere garantite in ogni circostanza, in particolare per quanto concerne i messaggi di posta scaricati sui

Personal Computer. In questo caso è indispensabile che l'utente stesso provveda ad attuare le azioni adeguate a proteggere le informazioni usando tutti i mezzi disponibili, quali ad esempio password di accesso alle applicazioni e alla propria postazione di lavoro5.

6.4. Posta Elettronica in caso di assenze programmate ed assenze non programmate

Nel caso di assenza prolungata sarebbe buona norma attivare il servizio di risposta automatica (Auto-reply). In alternativa, e in tutti i casi in cui sia necessario un presidio della casella di e-mail per ragioni di operatività aziendale, il Responsabile deve nominare un collega fiduciario con lettera scritta che in caso di assenza inoltri i file necessari a chi ne abbia urgenza. Qualora il Responsabile non abbia provveduto ad individuare un collega fiduciario o questi sia assente o irreperibile, l'organizzazione, mediante personale appositamente responsabile, potrà verificare il contenuto dei messaggi di posta elettronica dell'responsabile, informandone l'responsabile stesso e redigendo apposito verbale.

6.5. Utilizzo Illecito di Posta Elettronica

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

7 SEZIONE VII

USO DI ALTRI DISPOSITIVI (NOTEBOOK, TABLET, CELLULARE, SMARTPHONE E DI ALTRI DISPOSITIVI ELETTRONICI)

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

Il computer portatile, il tablet e il cellulare (di seguito generalizzati in "dispositivi mobili") possono venire concessi in uso dall'organizzazione ai Responsabili che durante gli spostamenti necessitino di disporre di archivi elettronici, supporti di automazione e/o di connessione alla rete dell'organizzazione. Il Responsabile è responsabile dei dispositivi mobili assegnatigli dall'organizzazione e deve custodirli con diligenza sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro. Ai dispositivi mobili si applicano le regole di utilizzo previste per i computer connessi in rete, con particolare attenzione alla rimozione di eventuali file elaborati sullo stesso prima della riconsegna. In particolare i file creati o modificati sui dispositivi mobili, devono essere trasferiti sulle memorie di massa aziendali al primo rientro in ufficio e cancellati in modo definitivo dai dispositivi mobili (Wiping). Sui dispositivi mobili è vietato installare applicazioni (anche gratuite) se non espressamente autorizzate dall'TITOLARE. I dispositivi mobili utilizzati all'esterno (convegni, visite in azienda, ecc...), in caso di allontanamento, devono essere custoditi in un luogo protetto. In caso di perdita o furto dei dispositivi mobili, deve far seguito la denuncia alle autorità competenti. Allo scopo si deve avvisare immediatamente l'TITOLARE che provvederà – se del caso – ad occuparsi delle procedure connesse alla privacy. Anche di giorno,

durante l’orario di lavoro, al Responsabile non è consentito lasciare incustoditi i dispositivi mobili. Al Responsabile è vietato lasciare i dispositivi mobili incustoditi e a vista dentro l’auto o in una stanza d’albergo o nell’atrio dell’albergo o nelle sale d’attesa delle stazioni ferroviarie e aeroportuali.

5

Vedi Politica PEO utenti scuola: ver.8 del 11.7.2016, MIUR

I dispositivi mobili che permettono l'attivazione di una procedura di protezione (PIN) devono sempre essere abilitabili solo con la digitazione del PIN stesso e non possono essere lasciti privi di PIN. Laddove il dispositivo mobile sia accompagnato da un'utenza, il Responsabile è chiamato ad informarsi preventivamente dei vincoli ad essa associati (es. numero minuti massimo, totale gigabyte dati, ...) e a rispettarli. Qualora esigenze lavorative richiedessero requirements differenti, il Responsabile è tenuto ad informare tempestivamente e preventivamente l'TITOLARE. In relazione alle utenze mobili, salvo autorizzazione dell'organizzazione, è espressamente vietato ogni utilizzo all'estero e anche in caso di autorizzazione dell'organizzazione, gli utilizzi all'esterno devono essere preventivamente comunicati all'organizzazione per permettere l'attivazione di opportuni contratti di copertura con l'operatore mobile di riferimento.

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

Ai Responsabili può essere assegnata una memoria esterna (quale una chiave USB, un hard disk esterno, una memory card, ...) su cui copiare temporaneamente dei dati per un facile trasporto, o altri usi (es. macchine fotografiche con memory card, videocamere con dvd, ...). Questi dispositivi devono essere gestiti con le stesse accortezze di cui all'articolo precedente e devono essere utilizzati esclusivamente dalle persone a cui sono state affidate e, in nessun caso, devono essere consegnate a terzi.

7.3. Dispositivi personali (BYOD).

Ai dipendenti non è permesso svolgere la loro attività su PC fissi, portatili, dispositivi personali se non per le finalità descritte di seguito.

Dispositivi ammessi: qualsiasi computer portatile, tablet, e-reader, smartphone;

• I dispositivi devono essere usati a scuola per soli scopi didattici e solo dopo previa autorizzazione esplicita del Dirigente, il quale amministra tempi e necessità di utilizzo di tali apparecchiature.

• È vietato agli studenti ed al personale usare dispositivi di registrazione audio, videocamere o fotocamere (o dispositivi che li prevedano) per registrare media o fare foto a scuola, senza il consenso esplicito dell'interessato, e solo dopo che il Dirigente ne ha autorizzato l'uso.

• Connessione alla rete Wi-Fi dell'TITOLARE: ogni lavoratore potrà usare la connessione wifi disponibile all'interno dell'TITOLARE solo per finalità didattiche o, comunque, istituzionali. Chi riceve le credenziali per l'accesso alla rete d'TITOLARE, avrà cura di conservarle in modo sicuro e l'obbligo di non diffonderle a terzi.

• Anche in considerazione di esigenze didattiche, il Dirigente Scolastico potrà autorizzare le classi aderenti a sperimentazioni in essere, temporaneamente o per l'intero anno scolastico, alla rete Wi-Fi d'TITOLARE.

Nel caso di utilizzo di dispositivi forniti dall'TITOLARE, è necessario che il dispositivo abbia password di sicurezza stringenti, approvate dall'TITOLARE e l'eventuale furto o smarrimento del dispositivo deve essere immediatamente segnalato anche all'TITOLARE, per eventuali provvedimenti di sicurezza. Al responsabile è vietato l'utilizzo di memorie esterne personali (quali chiavi USB, memory card, cd-rom, DVD, macchine fotografiche, videocamere, tablet, ...). I Responsabili non dipendenti (ovvero i consulenti e collaboratori esterni), possono utilizzare i propri dispositivi personali per memorizzare dati dell'TITOLARE solo se espressamente autorizzati dall'TITOLARE stesso e assumendone formalmente e

personalmente l’intera responsabilità del trattamento. Tali dispositivi dovranno essere preventivamente valutati dall’TITOLARE, per la verifica della sussistenza di misure minime ed idonee di sicurezza.

7.4. Utilizzo del cellulare/smartphone personale.

Durante l’orario di lavoro, comprese le eventuali pause, ai Responsabili è concesso l’utilizzo del telefono cellulare personale, ma solo per comunicazioni di emergenza o strettamente collegate all’ambito lavorativo. In caso di trasferte lavorative all’esterno degli uffici dell’organizzazione, il telefono personale può rimanere acceso, anche per facilitare la comunicazione con l’organizzazione stessa, ove fosse necessario. In questo caso si invita, comunque, a non utilizzarlo per fini personali, in modo particolare in presenza di clienti o fornitori.

I Responsabili non dipendenti (ovvero i consulenti e collaboratori esterni), possono utilizzare i propri cellulari/smartphone per memorizzare dati dell'TITOLARE solo se espressamente autorizzati dall'TITOLARE stesso e assumendone formalmente e personalmente l'intera responsabilità del trattamento. Tali cellulari/smartphone dovranno essere preventivamente valutati dall'TITOLARE, per la verifica della sussistenza di misure minime ed idonee di sicurezza.

7.5. Distruzione dei dispositivi

Ogni dispositivo ed ogni memoria esterna affidati ai responsabili, (computer, notebook, tablet, smartphone, memory card, chiavi usb, hard disk, dvd, cd-rom, ecc.), al termine del loro utilizzo dovranno essere restituiti all'TITOLARE, che provvederà a distruggerli o a ricondizionarli seguendo le norme di legge in vigore al momento. In particolare, l'TITOLARE provvederà a cancellare o a rendere inintelligibili i dati negli stessi memorizzati.

8 SEZIONE VIII

SISTEMI IN CLOUD

8.1. Cloud Computing

In informatica con il termine inglese cloud computing (in italiano nuvola informatica) si indica un paradigma di erogazione di risorse informatiche, come l'archiviazione, l'elaborazione o la trasmissione di dati, caratterizzato dalla disponibilità on demand attraverso Internet a partire da un insieme di risorse preesistenti e configurabili. Le risorse non vengono pienamente configurate e messe in opera dal fornitore apposta per l'utente, ma gli sono assegnate, rapidamente e convenientemente, grazie a procedure automatizzate, a partire da un insieme di risorse condivise con altri utenti lasciando all'utente parte dell'onere della configurazione. Quando l'utente rilascia la risorsa, essa viene similmente riconfigurata nello stato iniziale e rimessa a disposizione nel pool condiviso delle risorse, con altrettanta velocità ed economia per il fornitore. Utilizzare un servizio di cloud computing per memorizzare dati personali o sensibili, espone l'TITOLARE a potenziali problemi di violazione della privacy. I dati personali vengono memorizzati nelle server farms di aziende che spesso risiedono in uno stato diverso da quello dell'TITOLARE. Il cloud provider, in caso di comportamento scorretto o malevolo, potrebbe accedere ai dati personali per eseguire ricerche di mercato e profilazione degli utenti. Con i collegamenti wireless, il rischio sicurezza aumenta e si è maggiormente esposti ai casi di pirateria informatica a causa della minore sicurezza offerta dalle reti senza fili. In presenza di atti illegali, come appropriazione indebita o illegale di dati personali, il danno potrebbe essere molto grave per l'TITOLARE, con difficoltà di raggiungere soluzioni giuridiche e/o rimborsi se il fornitore risiede in uno stato diverso da paese dell'utente. Nel caso di industrie o aziende, tutti i dati memorizzati nelle memorie esterne sono seriamente esposti a eventuali casi di spionaggio industriale.

8.2. Utilizzo di sistemi cloud

È vietato ai responsabili l'utilizzo di sistemi cloud non espressamente approvati dall'TITOLARE. Per essere approvati, i sistemi cloud devono rispondere ad almeno i seguenti requisiti: – Essere sistemi cloud esclusivi e non condivisi. – Essere sistemi cloud posizionati fisicamente nell'Unione Europea. – L'azienda che fornisce il sistema in cloud deve essere preventivamente nominata Responsabile al

Trattamento dei dati da parte dell'TITOLARE. – L'azienda che fornisce il sistema in cloud deve

comunicare all’TITOLARE, almeno una volta all’anno, i

nominativi degli amministratori di sistema utilizzati. – Dovranno essere verificate tutte le indicazioni e prescrizioni previste dal Garante della Privacy nei

suoi provvedimenti sugli Amministratori di Sistema e sul cloud.

9 SEZIONE IX

GESTIONE DATI CARTACEI

9.1. Clear Desk Policy

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

I Responsabili sono invitati dall'organizzazione ad adottare una "politica della scrivania pulita". Ovvero si richiede agli responsabili di trattare dati cartacei solo se necessario, privilegiando, ove possibile, l'utilizzo degli strumenti digitali messi a disposizione dell'TITOLARE.

I principali benefici di una politica della scrivania pulita sono: – Una buona impressione a clienti e fornitori che visitano la nostra organizzazione. – La riduzione della possibilità che informazioni confidenziali possano essere viste da persone non

abilitate a conoscerle. – La riduzione che documenti confidenziali possano essere sottratti all'organizzazione.

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

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

A fine giornata, deve essere previsto il riordino della scrivania e la corretta archiviazione di tutte le pratiche d'ufficio, in modo da lasciare la scrivania completamente sgombra. Ove possibile, si invita ad evitare la stampa di documenti digitali, anche ai fini di ridurre l'inquinamento ed il consumo delle risorse in ottica ecologica.

Ove possibile, si invita ad effettuare la scansione dei documenti cartacei ed archiviarli digitalmente. È necessario rimuovere immediatamente ogni foglio stampato da una stampante o da un'apparecchiatura fax, per evitare che siano prelevati o visionati da soggetti non autorizzati. Ove possibile, è buona norma eliminare i documenti cartacei attraverso apparecchiature trita documenti.

10 SEZIONE X

APPLICAZIONE E CONTROLLO

10.1 Il controllo

Il TITOLARE, si riserva la facoltà di effettuare i controlli che ritiene opportuni per le seguenti finalità: – Tutelare la sicurezza e preservare l'integrità degli strumenti informatici e dei dati. – Evitare la commissione di illeciti o per esigenze di carattere difensivo anche preventivo. – Verificare la funzionalità del sistema e degli strumenti informatici.

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

10.2 PROTOCOLLO OPERATIVO IN CASO DI INCIDENTE

Qualora si ha conoscenza concreta di INCIDENTE su PERDITA di DATI PERSONALI, FURTO, MANOMISSIONE o INDISPONIBILITÀ' gli INCARICATI AL TRATTAMENTO sono obbligati a Comunicare al TITOLARE del TRATTAMENTO o suo incaricato ENTRO 24 ore l'ACCADUTO utilizzando gli appositi moduli disponibile nella sezione privacy della INTRANET o SITO Del titolare.

10.2. Modalità di verifica

In applicazione del principio di necessità di cui all'art. 3 del Codice Privacy, l'organizzazione 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 Responsabili e allo scopo ha adottato ogni possibile strumento tecnico, organizzativo e fisico, volto a prevenire trattamenti illeciti sui dati trattati con strumenti informatici. Il TITOLARE informa di non adottare sistemi che determinano interferenza ingiustificata sui diritti e sulle libertà fondamentali di lavoratori, come pure di soggetti esterni che ricevono o inviano comunicazioni elettroniche di natura personale o privata. In particolare, eventuali sistemi atti a monitorare eventuali violazioni di legge o comportamenti anomali da parte dei Responsabili avvengono nel rispetto del principio di pertinenza e non eccedenza, con esclusione di registrazioni o verifiche con modalità sistematiche. 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 file pirata, navigazioni da cui sia derivato il download di virus informatici, ecc.) si effettuerà un avvertimento in modo generalizzato con l'invito ad attenersi scrupolosamente ai compiti assegnati e alle istruzioni impartite.

10.3. Modalità di Conservazione

I sistemi software sono stati programmati e configurati in modo da cancellare periodicamente ed automaticamente i dati personali relativi agli accessi ad Internet e al traffico telematico, la cui conservazione non sia necessaria. Un eventuale prolungamento dei tempi di conservazione viene valutato come eccezionale e deve aver luogo solo in relazione: – 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.

11 SEZIONE XI

SOGGETTI PREPOSTI DEL TRATTAMENTO

11.1. Individuazione dei Soggetti autorizzati

Per quanto riguarda i soggetti preposti al connesso trattamento dei dati (in particolare, i responsabili della manutenzione) sono stati appositamente responsabili di svolgere solo operazioni strettamente necessarie al perseguimento delle finalità di sicurezza informatica, senza realizzare attività di controllo a distanza, neanche di propria iniziativa. I soggetti che operano quali amministratori di sistema o le figure analoghe cui siano rimesse operazioni connesse al regolare funzionamento dei sistemi, svolgono un'attività formativa sui profili tecnico- gestionali e di sicurezza delle reti, sui principi di protezione dei dati personali e sul segreto nelle comunicazioni.

12 SEZIONE XII

PROVVEDIMENTI DISCIPLINARI

12.1. Conseguenze delle infrazioni disciplinari

Le infrazioni disciplinari alle norme del presente Disciplinare Interno potranno essere punite, a seconda della gravità delle mancanze, in conformità alle disposizioni di legge e/o del Contratto Collettivo Nazionale del Lavoro applicato, tra cui: – Il biasimo inflitto verbalmente. – Lettera di richiamo inflitto per iscritto. – Multa. – La sospensione dalla retribuzione e dal servizio. – Il licenziamento disciplinare e con le altre conseguenze di ragioni e di legge; Per i dirigenti valgono le vigenti norme di legge e/o di contrattazione collettiva, fermo restando che, per le violazioni di maggior gravità l'Amministrazione potrà procedere al licenziamento del dirigente autore dell'infrazione.

12.2. Modalità di Esercizio dei diritti

Il lavoratore interessato del trattamento dei dati effettuato mediante strumenti informatici ha diritto di accedere, ai sensi dell'art. 15 del Regolamento, alle informazioni che lo riguardano scrivendo al Titolare dell'organizzazione.

13 SEZIONE XIII

VALIDITA', AGGIORNAMENTO ED AFFISSIONE

13.1. Validità

Il presente Disciplinare ha validità immediata dalla data di pubblicazione.

13.2. Aggiornamento

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

13.3. Affissione

Il presente Disciplinare verrà data AMPIA DIFFUSIONE, ai sensi dell'art. 7 della legge 300/70 e del CCNL.

il TITOLARE DEL TRATTAMENTO