Provvedimenti per uso dei servizi in rete

Elenco dei provvedimenti adottati per consentire l'utilizzo di servizi in rete, anche a mezzo di intermediari abilitati, per la presentazione telematica da parte di cittadini e imprese di istanze e atti, per la richiesta di attestazioni e certificazioni, nonché dei termini e modalità di utilizzo dei servizi e dei canali telematici e della posta elettronica.

Riferimenti normativi

DPR 13/11/2014 Regole tecniche in materia di formazione, trasmissione, copia, duplicazione, riproduzione e validazione temporale dei documenti informatici nonché' di formazione e conservazione dei documenti informatici delle pubbliche amministrazioni ai sensi degli articoli 20, 22, 23-bis, 23-ter, 40, comma 1, 41, e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005. (15A00107) (GU Serie Generale n.8 del 12-1-2015

DPR 318/1999 Regolamento recante norme per l'individuazione delle misure minime di sicurezza per il trattamento dei dati personali;

“Sicurezza informatica e delle telecomunicazioni nelle pubbliche amministrazioni” Direttiva 16 gennaio 2002;

"Codice in materia di protezione dei dati personali”, Decreto Legislativo 30 giugno 2003, n. 196;

“Codice dell’Amministrazione Digitale” Decreto Legislativo 7 marzo 2005, n.82;

“Linee Guida per la Pubblica Amministrazione Digitale”, Direttiva 18 novembre 2005;

“Linee guida del Garante per posta elettronica e internet”, Gazzetta Ufficiale n. 58 del 10 marzo 2007;

“Utilizzo di Internet e della casella di posta elettronica istituzionale sul luogo di lavoro”, Direttiva 02/09, Dipartimento della Funzione Pubblica

Utilizzo delle postazioni di lavoro (PDL)

Le PDL, sia da tavolo che portatili, sono predisposte con la necessaria dotazione di dispositivi (hardware) e programmi (software) tali da consentirne il loro corretto funzionamento in conformità a standard dell'Istituto e nel rispetto delle necessarie licenze d'uso. L'installazione e l'aggiornamento dei dispositivi e dei programmi è di esclusiva competenza del personale espressamente incaricato dalla Dirigente: è quindi vietato:

Installare software non autorizzato;

Modificare in parte o del tutto il software o le sue configurazioni di funzionamento;

Asportare o copiare in parte o del tutto il software;

Modificare, aggiungere o rimuovere dispositivi hardware;

Utilizzare strumenti software e/o hardware atti a interpretare, falsificare, alterare o sopprimere il contenuto di comunicazioni e/o documenti informatici;

Utilizzare dispositivi di comunicazione diversi da quelli di cui è dotata la PDL (es.: modem, switch, hub, router, telefoni cellulari e palmari, apparati di rete non autorizzati);

Disattivare o disinstallare, anche temporaneamente, il Sistema antivirus dell'Istituto (SEP);

Aprire sessioni di lavoro remote tramite PDL connesse alla Rete dell'Istituto;

Compromettere il funzionamento dei Servizi di Rete e degli apparecchi che li costituiscono con virus o programmi diretti a danneggiare od interrompere la continuità operativa;

Connettere alla rete dell'Istituto computer e/o apparati non preventivamente comunicati al DS o al DSGA;

Distruggere, deteriorare o rendere in tutto od in parte inutilizzabili programmi, informazioni o dati altrui;

Lasciare incustodita la stazione di lavoro se non in una condizione di spegnimento o blocco all'accesso.

Si sottolinea che il cosiddetto software "shareware" o "freeware" scaricabile da Internet è generalmente esente da licenza SOLO per uso amatoriale. L'utilizzo su stazioni di lavoro di una società deve essere subordinato alla formalizzazione della relativa licenza d'uso (ricadono in questa categoria software molto comuni quali: screensavers, compressori, "criptatori", ecc.), a tal proposito si richiama quanto già indicato nei punti precedenti. Ogni PDL alla quale il dipendente può accedere deve essere considerata come strumento di produttività, e come tale deve essere utilizzato, inoltre nei casi in cui la stazione di lavoro venga sottoposta a qualsiasi intervento di manutenzione, sia straordinario che dietro richiesta dall'utente, e vengano individuati software applicativi non riconducibili a tipiche installazioni dell'Ic San Polo il Responsabile sarà autorizzato alla rimozione di tali software dalla PDL ripristinandone le configurazioni iniziali.

Gestione dei dati trattati mediante strumenti elettronici

L'IC di Mareno di Piave e Vazzola adotta nell'ambito delle regole generali, un complesso di misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza volte ad assicurare un livello minimo di protezione di dati personali e sensibili. L'accesso dei dati trattati con l'ausilio di strumenti elettronici è disciplinato dalle seguenti misure e relative modalità di trattamento:

Autenticazione informatica;

Adozione di procedure di gestione delle credenziali di autenticazione;

Aggiornamento periodico della gestione e della manutenzione degli strumenti elettronici;

Protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti, accessi non consentiti e a determinati programmi informatici;

Adozione di procedure per la custodia di copie di sicurezza, il ripristino della disponibilità dei dati e dei sistemi;

Tenuta di un aggiornato documento programmatico sulla sicurezza;

Il trattamento di dati personali e/o sensibili con strumenti elettronici è consentito agli incaricati dotati di credenziali di autenticazione;

Le credenziali di autenticazione consistono in un codice per l'identificazione dell'incaricato (username) associato a una parola chiave (password) riservata conosciuta solamente dal medesimo oppure in un dispositivo di autenticazione in possesso e uso esclusivo dell'incaricato;

Ad ogni incaricato sono assegnate o associate individualmente una o più credenziali per l'autenticazione: le credenziali di autenticazioni sono strettamente personali e per questo non devono essere in alcun modo comunicate ad altri operatori;

Con le istruzioni impartite agli incaricati è prescritto di adottare le necessarie cautele per assicurare la segretezza della componente riservata della credenziale e la diligente custodia dei dispositivi in possesso ed uso esclusivo dell'incaricato;

La parola chiave, quando è prevista dal sistema di autenticazione, è composta da almeno otto caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito; essa non contiene riferimenti agevolmente riconducibili all'incaricato ed è modificata da quest'ultimo al primo utilizzo e, successivamente, almeno ogni sei mesi. In caso di trattamento di dati sensibili la parola chiave è modificata almeno ogni tre mesi;

Il codice per l'identificazione, laddove utilizzato, non può essere assegnato ad altri incaricati, neppure in tempi diversi;

Le credenziali di autenticazione non utilizzate da almeno sei mesi sono disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica;

Le credenziali sono disattivate anche in caso di perdita della qualità che consente al Responsabile l'accesso ai dati personali;

Sono state impartite istruzioni agli incaricati per non lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento;

Alla fine della sessione di lavoro eseguire le procedure di uscita (logout) dall'applicativo accertandosi della chiusura di tutte le finestre nelle quali sono evidenti dati personali e/o sensibili;

Abilitare sulle postazioni screen-saver automatici che intervengono dopo alcuni minuti di inattività: tali screen-savers devono richiedere all'utente la ri-immissione dello username e della password;

quando l'accesso ai dati e agli strumenti elettronici è consentito esclusivamente mediante uso della componente riservata della credenziale per l'autenticazione, sono impartite idonee e preventive disposizioni scritte volte a individuare chiaramente le modalità con le quali il titolare può assicurare la disponibilità di dati o strumenti elettronici in caso di prolungata assenza o impedimento dell'incaricato che renda indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema;

Le disposizioni sul sistema di autenticazione di cui ai precedenti punti e quelle sul sistema di autorizzazione non si applicano ai trattamenti dei dati personali destinati alla diffusione;

gli aggiornamenti periodici dei programmi per elaboratore volti a prevenire la vulnerabilità di strumenti elettronici e a correggerne difetti sono effettuati almeno annualmente. In caso di trattamento di dati sensibili o giudiziari l'aggiornamento è almeno semestrale;

Sono impartite istruzioni organizzative e tecniche che prevedono il salvataggio dei dati con frequenza almeno giornaliera/settimanale;

Gestione dei dati sulle stazioni di lavoro

Costituisce buona regola la pulizia periodica (almeno una volta l'anno) degli archivi, con cancellazione dei file obsoleti o ritenuti inutili. Particolare attenzione deve essere prestata alla duplicazione dei dati: è infatti assolutamente da evitare un'archiviazione ridondante al fine di salvaguardare spazio e permettere alla risorsa un'operatività costante ed efficiente nonché ridurre gli intervalli di manutenzione. Le gestioni locali dei dati dovranno essere ridotte al minimo per essere sostituite da gestioni centralizzate su server come indicato dalla normativa vigente. Nell'effettuare il trattamento dei dati personali devono essere soddisfatti i principali contenuti nella percepita normativa in materia di privacy e di sicurezza dei dati trattati. I dati personali devono esser esatti e, se necessario aggiornati nonché pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti o successivamente trattati. Il trattamento deve avvenire in modo lecito, e secondo correttezza; la raccolta e registrazione dei dati stessi deve avvenire per finalità non incompatibili con tali scopi. La conservazione deve avvenire per un periodo di tempo non superiore a quello

necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati. In particolare si deve osservare che le informazioni archiviate elettronicamente devono essere ridotte al minimo e riguardare esclusivamente quelle previste dalla legge, necessarie all'attività lavorativa secondo finalità determinate, esplicite e legittime, osservando il principio della pertinenza e non eccedenza.

Per altre misure vedere il piano per la PRIVACY

Utilizzo dei servizi di Rete

L'accesso ad Internet, attraverso la Rete dell'Istituto, è consentito per ragioni e finalità connesse ai compiti istituzionali del dipendente utilizzatore.

E' vietato l'utilizzo della rete internet per fini personali estranei all'attività lavorativa;

È fatto divieto assoluto di scaricare programmi, o contenuti multimediali senza la previa autorizzazione del Responsabile I.T.;

Non è consentita ogni genere di transazione finanziaria (acquisti/vendite on-line) e simili salvo casi direttamente autorizzati dalla DS o dal Dsga e con il rispetto delle normali procedure di acquisto;

Gli utenti sono invitati a limitare al massimo il rilascio d'informazioni personali durante la navigazione via Web. L'utente è tenuto, nel corso della navigazione, a leggere con attenzione qualsiasi finestra, pop-up o avvertenza prima di proseguire nella navigazione stessa e in particolare prima di accettare qualsivoglia condizione contrattuale o di aderire ad iniziative online;

Non è permesso l'uso della rete internet per attività ludiche;

Non è permessa la partecipazione, per motivi non professionali, a forum, l'utilizzo di chat-line, di bacheche elettroniche e le registrazioni in guest book anche utilizzando pseudonimi (o nickname);

Non è consentita la memorizzazione di documenti informatici di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza politica;

Il Responsabile della privacy, su autorizzazione della Dirigente, ha facoltà di porre limiti alla navigazione internet escludendo dalla navigazione siti non attinenti agli scopi scolastici.

E' tuttavia consentito l'utilizzo di internet per svolgere attività che non rientrano tra i compiti istituzionali per assolvere incombenze amministrative e burocratiche senza allontanarsi dal luogo di lavoro, ad esempio per effettuare adempimenti on-line nei confronti dei pubbliche amministrazioni e di concessionari di servizi pubblici ovvero per tenere rapporti con istituti bancari (home-banking, remote-banking) ed assicurativi, purché contenuto nei tempi strettamente necessari allo svolgimento delle transazioni.

Nel caso si verificasse la necessità di scaricare programmi o loro aggiornamenti dalla Rete (download), è necessario rivolgersi al Responsabile ed in ogni caso:

verificare il possesso dei necessari diritti d'uso;

verificare la presenza sulla PDL dell' adeguato software antivirus dell'Istituto (SEP);

Utilizzo della posta elettronica

La casella di posta elettronica, assegnata dall'Istituto all'utente, è uno strumento di lavoro. Le persone assegnatarie delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse. La comunicazione in forma elettronica, per scopi istituzionali, deve avvenire esclusivamente con l'utilizzo del sistema di posta elettronica dell'Istituto Comprensivo di Mareno di Piave e Vazzola ovvero non sono

consentiti l’utilizzo di comunicazioni effettuate da account differenti da quello dell'Istituto riferito all’utente e o al servizio (esempio @libero.it, @virgilio.it,…).

Nel caso in cui un utente fosse sprovvisto di casella personale, esso è tenuto a contattare il Responsabile al fine di colmare questa carenza. Ciascuna casella email viene fornita di una password di sola attivazione che l’utente avrà l’obbligo di modificare già dal suo primo accesso, per i dettagli tecnici dell’operazione di modifica contattare eventualmente il Responsabile o seguire le istruzioni riportate su aruba.it

La casella di posta elettronica dell'Istituto è consultabile laddove vi è una connessione Internet unicamente in modalità web raggiungendo l’indirizzo

https://webmail.aruba.it/.

Il servizio di posta elettronica è messo a disposizione degli utenti esclusivamente per attività connesse a fini istituzionali, esso è personale ed è vietato l’utilizzo della posta elettronica per scopi personali durante l'orario di lavoro; al di fuori dell'orario di lavoro e nelle pause ne è tollerato un utilizzo moderato. Tale utilizzo va effettuato utilizzando caselle nominative e non caselle di posta elettronica generiche dell'Istituto;

è completa responsabilità dell’utente la conservazione della password d’accesso, della sua gestione e della sua modifica ad intervalli periodici. Sono altresì previste apposite caselle istituzionali affidate alla responsabilità delle strutture di competenza; è' vietato:

utilizzare altri sistemi di posta, anche se offerti gratuitamente, diversi rispetto agli strumenti standard dell'Istituto (Webmail);

utilizzare le risorse informatiche per la comunicazione elettronica in modo anonimo o modificando la reale identità del mittente;

inviare a terzi, esterni all’Istituto, materiale di proprietà dell’Istituto Comprensivo di Mareno di Piave e Vazzola senza preventiva autorizzazione;

inviare messaggi o documenti con contenuti illeciti;

aderire o innescare “catene di Sant'Antonio”;

rispondere allo spam o a email il cui mittente sia di dubbia natura;

installare e/o configurare autonomamente account di posta elettronica alternativi e non direttamente riferibili all’Istituto Comprensivo di Mareno di Piave e Vazzola;

inviare messaggi non pertinenti alle attività scolastiche o comunicazioni non richieste (spamming);

è vietato l'invio per posta elettronica di password o codici di accesso, credenziali e/o client VPN;

utilizzare il sistema di posta e l'indirizzo di posta elettronica, forniti dall'Istituto Comprensivo, a fini personali;

intercettare, impedire od interrompere comunicazioni di altri utilizzatori sulla Rete ed installare apparecchiature idonee a tale scopo.

Nel caso in cui l’utente perdesse il diritto all’utilizzo della casella di posta elettronica ad esempio in seguito a cessazione della collaborazione, pensionamento, trasferimento, ecc.. la stessa verrà definitivamente disabilitata entro 60gg previa comunicazione (email) da parte del Responsabile e tutto il contenuto verrà automaticamente rimosso senza alcuna possibilità di recupero;

Non è consentito l'utilizzo dell'indirizzo di posta elettronica dell'Istituto per la partecipazione e/o iscrizione a dibattiti, mailing-list, forum, bacheche elettroniche non attinenti l'attività istituzionale fatto salvo la

preventiva autorizzazione da parte della Direzione. Poiché la posta elettronica diretta all'esterno della rete dell'Istituto è suscettibile di intercettazione da parte di estranei e talvolta malintenzionati non deve essere utilizzata per inviare documenti di lavoro riservati contenenti dati personali e/o sensibili, se tale necessità si manifesta si consiglia di attivare meccanismi di crittografia dei dati o di spedizione multiple al fine di ridurre i rischi derivanti dall'attività.

L'utilizzatore è responsabile della manutenzione della propria casella di posta elettronica ed avrà cura di:

controllate la posta regolarmente;

cancellare i messaggi non più utili;

non inviare messaggi contenenti dati personali e/o sensibili

Si ricorda inoltre:

la documentazione ricevuta o inviata resta di proprietà dell'Istituto;

l'Istituto si riserva di verificare, nei modi ed ai fini consentiti dalla legge, il rispetto delle modalità di utilizzo del servizio di posta, specificate in queste norme.

Va altresì ricordato che:

ll datore di lavoro metta a disposizione di ciascun lavoratore apposite funzionalità di sistema, di agevole utilizzo, che consentano di inviare automaticamente, in caso di assenze (ad es., per ferie o attività di lavoro fuori sede), messaggi di risposta contenenti le "coordinate" (anche elettroniche o telefoniche) di un altro soggetto o altre utili modalità di contatto della struttura. É parimenti opportuno prescrivere ai lavoratori di avvalersi di tali modalità, prevenendo così l'apertura della posta elettronica. In caso di eventuali assenze non programmate (ad es., per malattia), qualora il lavoratore non possa attivare la procedura descritta (anche avvalendosi di servizi webmail), il titolare del trattamento, perdurando l'assenza oltre un determinato limite temporale, potrebbe disporre lecitamente, sempre che sia necessario e mediante personale appositamente incaricato (ad es., l'amministratore di sistema oppure, se presente, un incaricato aziendale per la protezione dei dati), l'attivazione di un analogo accorgimento, avvertendo gli interessati;

in previsione della possibilità che, in caso di assenza improvvisa o prolungata e per improrogabili necessità legate all'attività lavorativa, si debba conoscere il contenuto dei messaggi di posta elettronica, l'interessato sia messo in grado di delegare un altro lavoratore (fiduciario) a verificare il contenuto di messaggi e a inoltrare al titolare del trattamento quelli ritenuti rilevanti per lo svolgimento dell'attività lavorativa. A cura del titolare del trattamento, di tale attività dovrebbe essere redatto apposito verbale e informato il lavoratore interessato alla prima occasione utile;

i messaggi di posta elettronica contengano un avvertimento ai destinatari nel quale sia dichiarata l'eventuale natura non personale dei messaggi stessi, precisando se le risposte potranno essere conosciute nell'organizzazione di appartenenza del mittente e con eventuale rinvio alla predetta policy datoriale.