Istituto Comprensivo Statale "*Rita Levi Montalcini*"
Via Fontanella 2 - 63821 Porto Sant'Elpidio (FM) - Tel. 0734 992287 - Fax 0734 801181
E-mail: apic83600e@istruzione.it - Pec: apic83600e@pec.istruzione.it
C.F.: 90055060447 - Cod.Univoco fatturazione elettronica: UF15IP
Sito web: www.iscmontalcini.edu.it

Prot. n./data *(vedi segnatura di protocollo)* Porto Sant'Elpidio

REGOLAMENTO IT DI ISTITUTO

approvato dal Consiglio di Istituto nella seduta del 28/10/2026 con delibera n. 43

CAPO I - Disposizioni generali

Art. 1. - Ambito di applicazione – Perimetro

1) Il presente Regolamento si applica a tutti gli utilizzatori dei sistemi e dei servizi IT dell'organizzazione compresi nel perimetro, corrispondente alla massima estensione della rete di comunicazione privata fino al firewall di connessione con la rete pubblica, includendo anche i sistemi collegati via Virtual Private Network (VPN) e i sistemi posizionati in zone demilitarizzate (DMZ), in colocation, in hosting, in housing o in cloud.
2) Sono compresi tutti gli elementi della catena tecnologica come le facility, il network, i sistemi server, il middleware, le applicazioni come anche i sistemi di gestione della sicurezza, il monitoraggio e il controllo, i dispositivi client come i personal computer, i thin client, le stampanti multifunzione, i centralini telefonici, i telefoni basati su tecnologia IP, gli smartphone e i tablet.
3) Sono escluse dal perimetro tutte le reti Wi-Fi di tipo guest (ad accesso gratuito per il pubblico).
4) Gli utilizzatori dei servizi pubblicati e accessibili da Internet sono esclusi dal perimetro se collegati attraverso connessioni esterne al perimetro (ad esempio sono esclusi coloro che visitano i siti web istituzionali, la sezione relativa agli obblighi di amministrazione trasparente).

Art. 2. - Applicazione del Regolamento IT

1) Gli utenti sono obbligati ad accettare e a conformarsi al presente Regolamento come condizione necessaria per l'accesso e l'utilizzo dei servizi e dei sistemi IT.
2) Il rispetto delle prescrizioni è il prerequisito per un impiego legittimo e ottimale dei servizi e dei sistemi IT, sia per il personale deputato alla gestione che per tutti gli utilizzatori.

Art. 3. – Definizioni

Ai fini del presente regolamento s'intende per:
1) Minaccia: qualcosa di potenzialmente pericoloso; possibile evento non desiderato che porta alla perdita di riservatezza, integrità o disponibilità delle informazioni;
2) Vulnerabilità: caratteristica dei sistemi e dei processi che identifica una fragilità, un

punto debole che in particolari condizioni, può comportare la perdita di riservatezza, integrità o disponibilità delle informazioni;
3) Contromisure: azioni di prevenzione e mitigazione delle vulnerabilità individuate al fine di limitare i rischi di perdita di riservatezza, integrità o disponibilità delle informazioni;
4) Rischio: probabilità che un evento si verifichi ovvero che una minaccia si trasformi in evento indesiderato e dannoso sfruttando una vulnerabilità;
5) Fonte di rischio: elemento tangibile o intangibile che possiede il potenziale intrinseco di originare il rischio singolarmente o in combinazione con altri elementi;
6) Evento sfavorevole: particolare insieme di circostanze in grado di modificare in modo negativo e contrario rispetto al normale comportamento di un sistema, ambiente, processo, flusso di lavoro o di una persona;
7) Conseguenza: Effetto diretto o indiretto di un evento;
8) Incidente alla sicurezza: Evento volontario o involontario attribuibile a una o più persone con associato un costo economico diretto (es. sostituzione del bene e interruzione del servizio) oppure indiretto (uso non autorizzato di informazioni, violazioni di legge, danni di immagine e reputazionali) che comporta una minaccia alla sicurezza;
9) Impatto (negativo): Stima delle potenziali perdite dirette o indirette associate a un rischio;
10) Credenziali di autenticazione: codice per l'identificazione dell'utilizzatore di un sistema o di un dispositivo associato a una parola chiave riservata, conosciuta solamente dal soggetto (spesso identificata come coppia login o codice utente e password) e che lo identificano univocamente;
11) Spam: ovvero spazzatura spesso associata alla posta elettronica (in inglese junk e-mail) che indica la ricezione di messaggi spesso indesiderati, ripetuti o monotematici (es. pubblicità) il cui mittente spesso è sconosciuto.

Art. 4. – Principi

1) I principi ispiratori del presente regolamento sono:
a) Tutela dei diritti, delle libertà e della dignità delle persone;
b) Garanzia della necessaria continuità operativa per la miglior cura possibile dei pazienti e il minor dispendio di energie (umane, tecnologiche, temporali ed economiche);
c) Tutela del patrimonio informativo dell'organizzazione e riduzione dei rischi connessi al trattamento dei dati e quindi della probabilità di:
i. Accessi illegittimi ai sistemi o agli applicativi;
ii. Modifiche indesiderate alle informazioni;
iii. Perdita della disponibilità dei dati;
d) Conformità normativa;
e) Riduzione della superficie di esposizione rispetto alle vulnerabilità ovvero le debolezze sistemiche trasformabili in un evento indesiderato nel caso si attui una minaccia;
f) Corretto bilanciamento tra usabilità e sicurezza, adottando contromisure basate sull'Analisi dei rischi;
g) Adozione della Regola del minimo privilegio rispetto alla finalità (separation of duties policy), in ottica di stratificazione dei profili e degli accessi;
h) Diritto alla disconnessione degli utilizzatori dai sistemi mobile al di fuori dell'orario di lavoro.

Art. 5. - Condotta e utilizzo etico dei servizi e dei sistemi IT

2) I sistemi e i servizi IT sono forniti agli utenti per condurre e supportare la missione dell'organizzazione, ovvero a tutte le attività legate agli ambiti tecnici ed amministrativi.
3) Gli utenti sono responsabili dell'utilizzo dei sistemi e dei servizi IT in modo

eticamente corretto, sicuro, legale e conforme al presente regolamento, tenendo nella massima considerazione i diritti, le libertà fondamentali, la sensibilità delle persone come anche gli obiettivi primari dell'organizzazione.
4) L'utilizzatore di sistemi e servizi IT è direttamente responsabile di tutte le attività effettuate con gli account dell'organizzazione ricevuti, con particolare riguardo alle informazioni inviate o richieste, caricate o visualizzate nel proprio personal computer, gestionale Nuvola o sito web dell'Istituto e non.
5) All'utilizzatore di sistemi e servizi IT sono tassativamente vietate le seguenti attività:
a. La creazione o la trasmissione di qualsiasi materiale o documento, in qualsiasi formato, che possa essere ragionevolmente ritenuto offensivo, diffamatorio o osceno;
b. La creazione o la trasmissione di materiale o documento in qualsiasi formato che possa ragionevolmente essere ritenuto suscettibile di molestare, intimidire, danneggiare o turbare qualcuno o qualcosa;
c. La trasmissione non autorizzata di documenti etichettati come confidenziali su canali o sistemi non sicuri o non omologati dai Sistemi Informativi dell'organizzazione;
d. L'invio di dati di tipo sensibili su canali non sicuri (un esempio di strumento da evitare per inviare dati sensibili è la posta elettronica dell'organizzazione, che viaggia in chiaro quando inviata ad altro dominio di posta; è da ritenersi invece accettabilmente sicuro l'invio ad altro utente di posta dello stesso dominio. In caso di dubbi è necessario contattare i Sistemi Informativi dell'organizzazione o adottare tecniche di criptazione con invio della chiave su altro media);
e. La creazione o la trasmissione di qualsiasi documento non riconducibile alle funzioni o ai compiti di competenza oppure estraneo alle attività dell'organizzazione;
f. L'accesso non autorizzato ai sistemi o ai servizi IT.

CAPO II – Strumenti

Art. 6. - Identificazione, autenticazione e autorizzazione

1) L'organizzazione implementa nella gestione dei sistemi e dei servizi IT, la famiglia di protocolli AAA basata sulle funzioni di Autenticazione, Autorizzazione, Accounting (v. articolo successivo).
2) L'accesso alla rete e ai sistemi dell'organizzazione è possibile soltanto se l'utilizzatore:
a) È stato prima di tutto identificato ovvero sono conosciute le sue generalità ed è stato dotato di credenziali utente (nome utente, password e/o PIN, SPID/CIE), soggette alle condizioni previste in questa sezione del Regolamento;
b) Effettua l'autenticazione tramite immissione delle credenziali, in modo che il sistema possa verificare se l'individuo è chi sostiene di essere, permettendone univoca identificazione;
c) È stato autorizzato ovvero è stato conferito il diritto ad accedere a specifiche risorse in base al ruolo ricoperto, al profilo e alle specifiche mansioni assegnate.
3) La responsabilità delle azioni effettuate utilizzando nome utente e password e/o PIN, SPID/CIE sarà attribuita in termini di responsabilità al soggetto titolare dell'account, a meno di comprovato illecito da parte di terzi. Sono escluse le attività di supporto autorizzate dagli stessi utilizzatori per interventi di manutenzione o assistenza tecnica.
4) Gli account di accesso del personale dipendente, dei consulenti esterni e dei fornitori sono di tipo nominativo e non riutilizzabile da altri soggetti, anche dopo la conclusione del rapporto di lavoro.
5) Il personale dei Sistemi Informativi specificatamente autorizzato gestisce gli account utente per tutto il ciclo di vita tramite apposita procedura (creazione, aggiornamento, nuovi profili di autorizzazione, reset della password, disattivazione una

volta concluso il rapporto di lavoro).
6) La normativa vigente in tema di protezione dei dati, le norme volontarie e le best practice di settore impongono di stratificare le possibilità di accesso ai sistemi e ai servizi IT al fine di garantire un adeguato livello di sicurezza. Ad ogni account utente è collegato uno specifico profilo di autorizzazione che permette al singolo utilizzatore l'accesso in funzione del proprio ruolo, delle attività a cui è delegato e specificatamente autorizzato da un superiore (o soggetto Designato ai sensi del D.lgs. 196/03 e ss.mm.ii.). Le eventuali estensioni o eccezioni devono essere autorizzate e tracciate secondo procedura.
7) Il sistema di Autenticazione, Autorizzazione e Registrazione degli accessi ha l'obiettivo di garantire un adeguato livello di sicurezza, conforme a quanto previsto dalla normativa vigente e dal presente regolamento, poiché traccia, separa gli accessi nei livelli previsti, tutelando la riservatezza e l'integrità delle informazioni trattate.
8) In conformità alla normativa vigente, la politica di sicurezza dell'organizzazione prevede la necessità di accesso al gestionale Nuvola tramite autenticazione a più fattori (MFA) tramite le modalità multiple previste dai sistemi (SPID/CIE).

Art. 7. - Corretto uso delle Credenziali di autenticazione

1) Le credenziali di autenticazione (SPID/CIE per Nuvola e nome utente e password per account Gmail-Google Workspace) sono composte da un codice (account utente) e da una password e/o PIN conosciuti al solo utilizzatore. È tassativamente vietato rivelare la propria password di accesso alla rete, agli applicativi o servizi disponibili (inclusi i siti e le applicazioni ministeriali), anche a terzi autorizzati. Qualsiasi azione effettuata utilizzando account utente e password e/o PIN e SPID/CIE sarà attribuita in termini di responsabilità all'utente titolare registrato, a meno di comprovato illecito da parte di terzi.
2) La lunghezza minima della password deve essere di un numero congruo caratteri; considerato che i sistemi di violazione impiegano tempistiche esponenzialmente proporzionali con la lunghezza della password da violare, è necessario considerare almeno 14 caratteri per gli account dei servizi on-line (es. posta elettronica, piattaforme web) e per gli account qualificati amministrazione di sistema (Misura minima prevista da AgID - «Misure minime di sicurezza ICT per le pubbliche amministrazioni (Direttiva del Presidente del Consiglio dei ministri 1° agosto 2015)»).
3) Le password non devono essere trascritte; per questo è importante che siano facili da ricordare. È consigliabile utilizzare tecniche di memorizzazione.
4) È fondamentale utilizzare password diverse per scopi, piattaforme o applicativi diversi. L'eventuale violazione di un sistema potrebbe comportare effetti indesiderati anche su tutti gli altri sistemi utilizzati, dell'organizzazione e personali, riconducibili allo stesso soggetto.
5) Le password devono essere modificate ad intervalli regolari per ridurre l'eventuale finestra temporale di esposizione e comunque almeno ogni 3 mesi (cd. Password aging).
6) Le password non devono mai far riferimento a termini di senso compiuto poiché già contenute nei dizionari utilizzati dai sistemi di violazione, oppure essere troppo ovvie.
7) Le password non devono essere in alcun modo collegate alla vita privata o lavorativa dell'utilizzatore. Sono quindi da escludere i nominativi dei familiari, la data di nascita, il codice identificativo, la targa dell'auto, la squadra del cuore, il soprannome, ecc. (il precedente elenco non è esaustivo).
8) Le password devono contenere combinazioni di caratteri Maiuscoli, minuscoli, numeri e caratteri speciali (!, £, $, %, &, /, =, ?, §, @, #, …) anche quando non specificatamente richiesto dal sistema utilizzato (criteri di complessità).
9) Le password non devono essere riutilizzate a breve distanza di tempo; la rotazione minima prevista è almeno pari a 5 password diverse consecutive (cd. Password history);
10) Le password degli account di accesso ai sistemi non sottoposti alle politiche di complessità, di invecchiamento o di rotazione impostate nel sistema di autenticazione

centrale, devono comunque rispettare le medesime regole, agendo manualmente.
11) Le password e i PIN non devono essere comunicati a nessuno, per nessun motivo, con nessun mezzo. In caso di problemi di accesso alle risorse fare riferimento al supporto tecnico.
12) La digitazione delle password deve avvenire in massima sicurezza evitando di mostrare a terzi la sequenza dei tasti premuti.
13) I colleghi impegnati in attività condivise al computer sono tenuti a voltarsi nel caso sia richiesta l'autenticazione al sistema o alla piattaforma software utilizzati.
14) È vietata la memorizzazione delle password nei browser o tramite applicativi di gestione password (es. Pocket Password). Sono esclusi sistemi o applicativi software di memorizzazione delle credenziali nel cloud.
15) Non utilizzare strumenti web per la generazione o il controllo del livello di sicurezza (utilizzare eventualmente password con costruzione simile al solo fine di verificarne la robustezza; es. https://password.kaspersky.com/it).
16) Per l'invio delle password di criptazione dei file e della documentazione non utilizzare mai lo stesso canale (es. file criptato inviato via posta elettronica e password comunicata a voce, via telefono).
17) Non seguire le mode del momento, utilizzare acronimi, pattern, ripetizioni e sequenze o parole presenti nei dizionari (in Appendice 1 - Password presenti nei dizionari pubblici sono riportati degli esempi di password da NON utilizzare).
18) Nel caso di perdita (o anche solo il sospetto di perdita) della segretezza della password è necessario:
a. Modificare immediatamente la password in uso (sui sistemi Windows CTRL+ALT+CANC e Cambia password; verificare le modalità per i singoli applicativi software con autenticazione locale);
b. Comunicare l'accaduto ai Sistemi Informativi dell'organizzazione e alla Dirigenza per la valutazione della gravità della situazione e l'attivazione delle procedure di emergenza per incidente alla sicurezza, al fine di attivare tutti i controlli e le contromisure del caso.
19) Nei casi di particolare emergenza oppure in presenza di comportamenti che possano comportare problemi di sicurezza, i Sistemi Informativi sono autorizzati alla momentanea disattivazione dell'account e del sistema utilizzato. Risolta la problematica evidenziata sarà cura dei Sistemi Informativi ripristinare le precedenti autorizzazioni.
20) È tassativamente vietato memorizzare account di accesso ai sistemi e servizi dell'organizzazione in documenti salvati in sistemi o dispositivi al di fuori del perimetro dell'organizzazione e ad accesso pubblico, inclusi sistemi di file hosting (come Google Drive o Dropbox).

Art. 8. - Posta elettronica (Gmail di Istituto)

1) La posta elettronica è uno strumento di comunicazione e deve essere utilizzato soltanto per effettuare corrispondenze legate al servizio svolto nell'organizzazione.
2) Ogni utilizzo della posta elettronica deve essere effettuato coerentemente con le politiche e le procedure dell'organizzazione nel rispetto dell'etica, della sicurezza e in piena conformità alle leggi applicabili.
3) La posta elettronica non deve essere utilizzata per la creazione, distribuzione o rilancio di messaggi di disturbo o offensivi, commenti sull'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, lo stato di salute o la disabilità, il genere, il colore dei capelli, l'età, la vita o l'orientamento sessuale della persona. I dipendenti che dovessero ricevere messaggi con queste tipologie di contenuto da qualsiasi dipendente devono segnalare immediatamente la questione alla Dirigenza.
4) La posta elettronica ordinaria o e-mail secondo la recente giurisprudenza , rispetto

a quanto previsto dal Regolamento (UE) 2014/910 eIDAS (electronic IDentification Authentication and Signature) e dalle conseguenti modifiche al D.lgs. n. 82/2005 CAD (Codice dell'Amministrazione Digitale) ha validità giuridica e rilevanza probatoria , è liberamente valutabile in giudizio, tenuto conto delle sue caratteristiche oggettive di qualità, sicurezza, integrità e immodificabilità.

5) Alla fine della sessione di lavoro è necessario effettuare sempre la disconnessione (logout) dal sistema di posta.

6) L'indirizzo di posta elettronica non deve essere utilizzato per la registrazione a siti web che non siano in qualche modo legati alle attività istituzionali svolte dagli utilizzatori intestatari nell'organizzazione, anche al fine di limitare lo spam.

7) Non lanciare mai i link di annullamento alle sottoscrizioni delle e-mail considerate indesiderate (il cd. "unsubscribe"), al fine di ridurre il rischio di conferma dell'esistenza e utilizzo della e-mail.

8) I sistemi di sicurezza come firewall e antispam garantiscono con discreta probabilità che le e-mail consegnate siano esenti da pericoli. È sempre a carico dell'utilizzatore la verifica ultima di:

a. Mittente: deve essere conosciuto (da verificare l'indirizzo effettivo e non la semplice denominazione);

b. Link: i link devono essere verificati prima di essere lanciati anche nel caso appaiano a prima vista del tutto familiari (soprattutto come aspetto grafico) al fine di evitare attacchi di tipo phishing;

c. Allegati: diffidare dei file con estensione multipla o senza estensione o con denominazione estranea alle attività o mansioni svolte abitualmente;

d. Contenuti: scrittura con errori grossolani (traduzione da sistemi automatici), riferimenti alla chiusura di un conto o di un servizio, parole come URGENTE, richieste di dati personali o di password, file che non sono mai stati richiesti o con estensioni sospette.

9) Nei casi dubbi non aprire le e-mail o i contenuti e contattare il supporto tecnico che provvederà alla verifica secondo le procedure di sicurezza.

10) L'utilizzo di forward di posta automatico dell'organizzazione su altri sistemi è vietato; questo al fine di garantire un adeguato livello di sicurezza dei contenuti dei messaggi come, ad esempio, gli allegati contenenti dati personali o riservati inviati dal mittente.

11) La posta elettronica fornita dall'organizzazione non può essere utilizzata per scopi personali estranei all'attività lavorativa.

12) Non consultare la posta elettronica dell'organizzazione presso Internet point, Wi-Fi pubblici o sistemi di connettività condivisa (es. alberghi, ristoranti, bar).

13) Marcare come spam le e-mail che appaiono come scam ovvero tentativi di truffa pianificata con metodi di ingegneria sociale.

14) Le e-mail che richiedono l'attivazione delle macro di MS-Word o MS-Excel prima del download degli allegati devono essere immediatamente marcate come spam.

15) Non rispondere e inoltrare e-mail delle cosiddette "catene di Sant'Antonio" o rispondere alle e-mail di spam.

16) Gli allegati inviati via e-mail contenenti dati personali o riservati devono essere criptati adottando le procedure e le modalità previste in questi casi. La password di decriptazione deve essere comunicata al destinatario con altro mezzo (es. via telefono).

17) L'invio a più soggetti di un messaggio di posta elettronica può essere effettuato in "CC" (Copia Carbone) soltanto nel caso di destinatari appartenenti allo stesso dominio dell'Istituto; nel caso di invio a più destinatari è fondamentale utilizzare il "CCN" (Copia Carbone Nascosta) in modo che i singoli non possano in nessun modo venire a conoscenza degli indirizzi degli altri destinatari.

18) Dopo la cessazione del rapporto di lavoro dell'utilizzatore, l'account di posta elettronica verrà disabilitato dal team digitale di Istituto.

19) In nessun caso è possibile richiedere copia delle e-mail inviate o ricevute poiché relative al patrimonio informativo dell'organizzazione e contenenti comunicazioni

esclusivamente legate al rapporto di lavoro.
20) I documenti che generano, o fanno parte di, processi che hanno valenza amministrativa nonché quelli aventi efficacia esterna rispetto all'organizzazione (come determine, delibere, decreti, verbali, circolari e contratti), in quanto documenti di preminente carattere giuridico-probatorio e fondamentali per la gestione dei procedimenti amministrativi, possono essere inviati via posta elettronica soltanto dopo essere stati oggetto di registrazione di protocollo.
21) Per quanto qui non esplicitato, si rimanda al Regolamento di utilizzo e condizioni d'uso delle piattaforme digitali consultabile sul sito dell'Istituto Comprensivo "Rita Levi Montalcini".

Art. 9. - Navigazione Internet

1) È vietato navigare in orario di servizio per fini ludici o personali, effettuare upload o download di file e documenti non connessi all'attività lavorativa, effettuare streaming audio o video (es. radio o tv via Internet), telefonare (es. Skype), effettuare chat on-line se non specificatamente autorizzate.
2) È tassativamente vietata la navigazione in siti Internet palesemente incompatibili con le finalità dell'organizzazione, che istighino a comportamenti illegali, che consentano o siano a rischio di diffusione di virus, cavalli di Troia o di altri programmi il cui obiettivo sia la distruzione, alterazione, sabotaggio, intercettazione, hacking o pirateria informatica a danno dei computer di altri utenti interni o esterni al perimetro dell'organizzazione.
3) È inoltre vietato navigare in siti web che possano comportare nei sistemi deputati al monitoraggio e alla protezione della connessione Internet, trattamenti involontari di dati personali di tipo sensibile riconducibili agli utilizzatori del servizio (esempio convinzioni religiose, politiche, stato di salute, vita sessuale).
4) La navigazione web non è esente da rischi, nonostante siano già attivi diversi strumenti di protezione; gli impatti potrebbero non essere legati al singolo computer ma interessare parte o addirittura l'intero patrimonio informativo dell'organizzazione, con risvolti imprevedibili sulla continuità stessa dei servizi e danni reputazionali e di immagine. Per queste motivazioni è sempre in capo al singolo utilizzatore la verifica di:
a. Indirizzo del sito web: è necessario verificare più di una volta l'indirizzo completo (attenzione ai siti web che appaiono simili ma non lo sono);
b. Certificato: evitare i siti non sicuri (con protocollo http) e nel caso di siti in https fare attenzione alla perfetta corrispondenza del certificato con intestazione e indirizzo del sito web in questione;
c. Riferimenti: i siti dei cosiddetti scammer o truffaldini non riportano né l'indirizzo della sede né tantomeno numeri telefonici o altri riferimenti;
d. Link: i link devono essere verificati prima di essere lanciati anche nel caso appaiano a prima vista del tutto familiari (soprattutto nell'aspetto grafico); questo al fine di evitare attacchi di tipo phishing;
e. Download: evitare di scaricare da siti non ufficiali qualsiasi documento, software applicativo, driver o componente aggiuntivo (plug-in del browser o componenti "dinamici" come ActiveX o funzioni JavaScript), includendo anche le app per dispositivi mobile;
f. Contenuti: verificare la presenza di errori sintattici grossolani (dovuti a traduzione automatiche) al fine di riconoscere siti non ufficiali (tecnicamente denominati fake);
5) I rischi derivanti dall'utilizzo delle informazioni personali (ad es. numeri di carte di credito) durante la navigazione web estranea alle attività lavorative, sono sempre in capo all'utilizzatore. Il Titolare non potrà essere ritenuto responsabile di eventuali danni dovuti a perdite di riservatezza, integrità o disponibilità di dati personali inviati in sessioni effettuate con strumenti dell'organizzazione e in orario di lavoro.
6) L'acquisizione, conservazione, trasmissione o diffusione di file dal contenuto illegale, discriminatorio per origine razziale o etnica, opinioni politiche, convinzioni religiose

o filosofiche, o appartenenza sindacale, stato di salute o disabilità, genere, colore dei capelli, età, vita sessuale o orientamento sessuale della persona è vietato. Eventuali abusi o contenuti illegali che si dovessero evidenziare durante la navigazione devono essere comunicati al supporto tecnico per le valutazioni del caso.
7) L'acquisizione, conservazione, trasmissione o diffusione di materiale che violi il diritto d'autore, i marchi, i segreti commerciali o i diritti di brevetto di qualsiasi persona o organizzazione è vietato. Tutti i materiali pubblicati su Internet sono protetti da copyright e/o brevettati, salvo diversa indicazione (Legge 633/1941 – "Protezione del diritto d'autore e di altri diritti connessi al suo esercizio).
8) La trasmissione di informazioni proprietarie, riservate o altrimenti sensibili, contenenti dati personali di tipo particolare è vietata. Solo se specificatamente autorizzato, l'utente può effettuare l'invio/upload a condizioni di adottare controlli specifici e livelli di protezione elevati forniti dalla criptazione.

Art. 10. - Utilizzo del personal computer (desktop) o del portatile (laptop) di proprietà dell'Istituto

1) La continuità dei servizi è strettamente legata alla normale operatività di tutti i dispositivi della catena tecnologica, a partire dalla postazione di lavoro. Utilizzi impropri dei dispositivi e delle apparecchiature possono produrre effetti indesiderati e compromettere il funzionamento che, in casi particolari, potrebbe causare danni alle persone.
2) È vietato modificare la posizione, la configurazione hardware e software, la modalità di collegamento alla rete dell'organizzazione e all'alimentazione elettrica, da parte dell'utilizzatore o di personale esterno, senza specifica autorizzazione del personale del servizio di supporto tecnico.
3) Non è consentito l'uso o l'installazione di software applicativi senza specifica autorizzazione del personale del servizio di supporto tecnico.
4) È vietato conservare nei sistemi e unità di memorizzazione assegnati, file, documenti, e-mail, immagini, video non legati alle finalità lavorative e professionali, in particolar modo se di contenuto osceno o violento, offensivo alla morale o alla pubblica decenza, oltraggioso e/o discriminatorio.
5) Per quanto riguarda l'eventuale trasporto al di fuori del perimetro dell'organizzazione di dispositivi di memorizzazione contenenti dati personali e sensibili, la responsabilità in caso di perdita, smarrimento e involontaria diffusione dei dati contenuti nel dispositivo durante il trasporto al di fuori degli uffici, sarà attribuita all'utente titolare registrato.
6) L'utilizzatore di sistemi e servizi IT è invitato alla immediata segnalazione al servizio di supporto tecnico di eventuali danni, perdita di funzionalità parziale o totale dei dispositivi o delle apparecchiature.
7) Eventuali specifiche indicazioni o istruzioni fornite dal personale di supporto tecnico devono essere rispettate al fine di garantire il miglior funzionamento possibile dei sistemi, dei dispositivi e delle risorse condivise.
8) Concluse le attività lavorative o nel caso di momentanea assenza o allontanamento dalla postazione di lavoro, l'utilizzatore di sistemi e servizi IT è tenuto alla disconnessione dei servizi e degli applicativi attivi o alla completa disconnessione/arresto del sistema.

Art. 11. - Cloud computing e servizi IT esterni

L'utilizzo di sistemi basati su tecnologia cloud o web non autorizzati e tracciati è considerato un data breach con tutti i risvolti sanzionatori ed eventualmente risarcitori a carico dell'utilizzatore.

Art. 12. - Pubblicazione di informazioni sui siti web istituzionali e Social media

1) Il ISC Rita Levi Montalcini Porto Sant'Elpidio utilizza i propri siti web e i social media con finalità istituzionali e di interesse generale per informare, comunicare, ascoltare e per consentire una relazione più diretta e una maggiore partecipazione dell'utenza alle attività svolte.
2) Attualmente la comunicazione del ISC Rita Levi Montalcini Porto Sant'Elpidio avviene attraverso le pagine tematiche presenti su:
a. https://iscmontalcini.edu.it/
b. Facebook
c. Instagram
d. YouTube.
3) I contenuti che sono pubblicati sui siti web istituzionali e sui social possono comprendere comunicazioni sulle attività e i servizi erogati, comunicati stampa, pubblicazioni e documenti ufficiali, novità normative, informazioni su iniziative ed eventi di settore, immagini e video istituzionali e relativi a eventi a cui l'organizzazione partecipa.
4) I commenti e i post degli utenti, presentati preferibilmente con nome e cognome non fittizi, rappresentano l'opinione dei singoli e non quella dell'organizzazione, che non può essere ritenuta responsabile della veridicità o meno di ciò che viene postato sui canali da terzi, entità giuridiche o naturali.
5) I partecipanti alle discussioni sui social network sono responsabili dei contenuti pubblicati e delle opinioni espresse. Non sono comunque tollerati insulti, volgarità, offese, minacce. Devono essere evitati riferimenti a fatti o a dettagli privi di rilevanza pubblica, atteggiamenti violenti, offensivi o discriminatori rispetto al genere, orientamento sessuale, età, religione, convinzioni personali, origini etniche, disabilità. Messaggi contenenti dati personali (indirizzi e-mail, numeri di telefono, numeri di conto corrente, indirizzi, etc.), o dati di tipo particolare, come anche informazioni riservate o confidenziali relative all'organizzazione, saranno rimossi a tutela delle persone interessate.
6) Non sono tollerati comportamenti da cosiddetti hater, con insulti, turpiloquio, minacce o atteggiamenti che ledano la dignità personale, i diritti delle minoranze e dei minori, i principi di libertà e uguaglianza o altri principi costituzionalmente riconosciuti ed in particolare:
a. Contenuti che promuovono, favoriscono, o perpetuano la discriminazione sulla base del sesso, della razza, della lingua, delle opinioni politiche, credo religioso, età, stato civile, nazionalità, disabilità fisica o mentale, orientamento sessuale;
b. Contenuti sessuali o link (collegamenti) a contenuti sessuali;
c. Pubblicità evidente o sollecitazioni commerciali;
d. Incoraggiamento ad attività illecite;
e. Informazioni che possono tendere a compromettere la sicurezza o la sicurezza dei sistemi pubblici;
f. Contenuti che violino l'interesse di una proprietà legale o di terzi;
g. Commenti o post che presentino dati sensibili in violazione della normativa sulla protezione dei dati personali

Art. 13. - Gestione di una conference call (Etiquette Rules)

1) In una riunione tramite strumenti informatici valgono le stesse regole di educazione di una riunione convenzionale frontale. Vi sono però dei vincoli e dei possibili problemi legati alle tecnologie che richiedono una particolare attenzione al fine di evitare perdite di tempo e insoddisfazione dei partecipanti.
2) Nel caso in cui un partecipante sappia in anticipo di un probabile ritardo, è tenuto a comunicarlo all'organizzatore in modo che, se possibile, la call venga fissata in un secondo momento o posticipata;
3) Tutti i partecipanti alla call devono prestare attenzione al luogo da dove viene

effettuata la chiamata, ovvero in ambiente tranquillo, senza rumori di fondo e sempre supportati da una buona connettività sono esclusi luoghi pubblici, in presenza di altre persone anche se familiari, specie nel caso di trattazione di temi dell'organizzazione, delicati o comunque sottoposti a segreto di ufficio;

4) Ad esclusione dell'organizzatore, tutti i partecipanti si accertano di tenere chiusa (in modalità mute) la comunicazione audio in modo da evitare rumori di fondo o effetti Larsen (feedback acustico o più ritorno); il passaggio da muto a microfono attivo è effettuato dal partecipante solo in caso di richiesta di intervento o per richiedere la parola.

CAPO III – Attori e ruoli

Art. 14. - Utilizzatore dei servizi e degli applicativi

Gli utilizzatori dei servizi e degli applicativi hanno l'obbligo di segnalare immediatamente al proprio Dirigente qualsiasi evento o situazione di rischio della sicurezza dei sistemi e delle reti di comunicazione, al fine di tutelare il patrimonio informativo dell'organizzazione e garantire la necessaria continuità operativa.

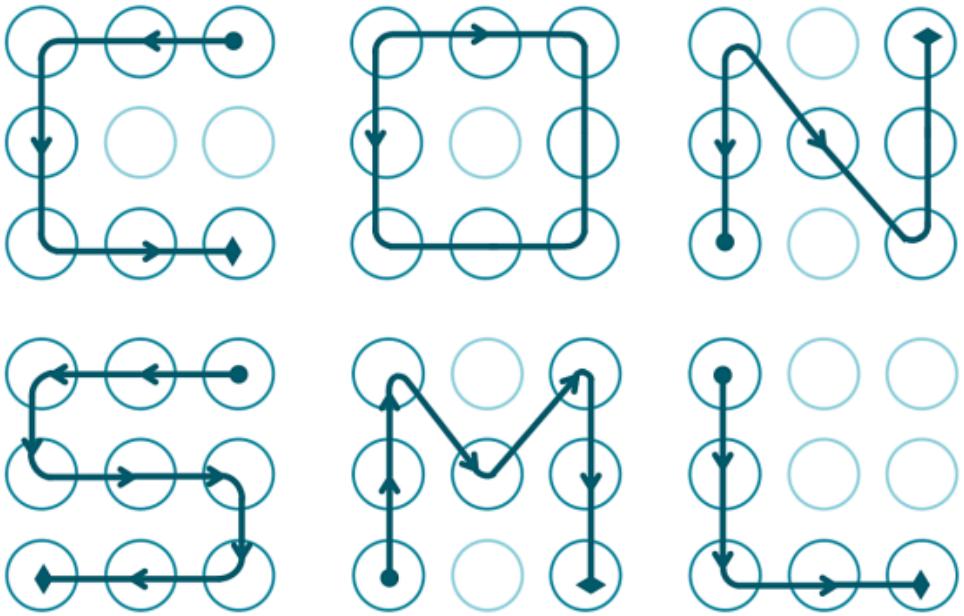
Appendice 1 - Password presenti nei dizionari pubblici

In ordine di frequenza rilevata:

Password	123456	123456789	Qwerty	password
1111111	12345678	abc123	1234567	1234567890
9876543210	password1	12345	letmein	football
iloveyou	admin	welcome	monkey	login
starwars	123123	dragon	passw0rd	master
hello	freedom	whatever	qazwsx	trustno1

Le password riportate in questo elenco NON DEVONO essere utilizzate.

Appendice 2 – Combinazioni “FACILI” di sblocco smartphone e tablet



Le combinazioni di sblocco riportate in questo elenco NON DEVONO essere utilizzate.

PIN più utilizzati (4 cifre)

1234	1111	0000	1212
7777	1004	2000	4444
2222	6969	9999	3333
5555	6666	1122	1313
8888	4321	2001	1010

I PIN riportati in questo elenco NON DEVONO essere utilizzati.