Disciplinare tecnico per l'utilizzo degli strumenti di lavoro

adottato da

Istituto d'istruzione Secondaria Superiore

"*J. von Neumann*"

sede centrale: Via Pollenza, 115 - 00156 ROMA
succursale: Via del Tufo, 27 - 00158 ROMA

Indice

1. Entrata in vigore del regolamento e pubblicità

1.1 Con l'entrata in vigore del presente regolamento tutte le disposizioni in precedenza adottate in materia, in qualsiasi forma comunicate, devono intendersi abrogate e sostituite dalle presenti.

2. Campo di applicazione del regolamento

2.1 Il regolamento si applica a tutti i lavoratori, ossia ai dipendenti, senza distinzione di ruolo e/o livello, nonché a tutti i collaboratori dell'IISS J. VON NEUMANN a prescindere dal rapporto contrattuale con la stessa intrattenuto (lavoratori somministrati, collaboratore a progetto, in stage, ecc.).

2.2 Ai fini delle disposizioni dettate per l'utilizzo delle risorse informatiche e telematiche, per "utente" deve intendersi ogni lavoratore in possesso di specifiche credenziali di autenticazione. Tale figura sarà anche indicata quale "autorizzato del trattamento" nell'accezione propria dell'art. 29 del GDPR.

3. Utilizzo del Personal Computer

3.1 **Il Personal Computer affidato all'utente è uno strumento di lavoro**. Ogni utilizzo non inerente all'attività lavorativa può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza. Il personal computer (PC) deve essere custodito con cura evitando ogni possibile forma di danneggiamento.

1.2 Il personal computer dato in affidamento all'utente permette l'accesso alla rete di IISS J. VON NEUMANN solo attraverso specifiche credenziali di autenticazione come meglio descritto al successivo punto 4 del presente Regolamento.

3.3 Il personale autorizzato che opera presso il servizio Area Servizi Informatici o altra figura dell' IISS J. VON NEUMANN e preposta alla gestione del sistema informatico dell' IISS J. VON NEUMANN (nel seguito per brevità "Servizio ICT"), per l'espletamento delle sue funzioni e per garantire la sicurezza del sistema informatico, ha la facoltà, in qualunque momento, di accedere ai dati trattati da ciascuno, ivi compresi gli archivi di posta elettronica, come più specificatamente precisato al successivo punto 13.1 del presente regolamento. La stessa facoltà, sempre ai fini della sicurezza del sistema e per garantire la normale operatività si applica anche in caso di assenza prolungata od impedimento dell'utente. Analoghe verifiche possono essere effettuate sui siti internet acceduti dagli utenti abilitati alla navigazione esterna. L'accesso, comunque, verrà effettuato con modalità tali da evitare qualsiasi forma di controllo a distanza. In ogni caso, l' IISS J. VON NEUMANN garantisce la non effettuazione di alcun trattamento mediante sistemi *hardware* e *software* specificatamente preordinati al controllo a distanza, quali, a titolo esemplificativo:

- lettura e registrazione sistematica dei messaggi di posta elettronica ovvero dei relativi dati esteriori, al di là di quanto tecnicamente necessario per svolgere il servizio *e-mail*;
- riproduzione ed eventuale memorizzazione sistematica delle pagine *web* visualizzate

dal lavoratore;
- la lettura e la registrazione dei caratteri inseriti tramite la tastiera o analogo dispositivo;
- l'analisi occulta di computer portatili affidati in uso.

3.4 Il personale autorizzato del servizio ICT ha la facoltà di collegarsi e visualizzare in remoto il desktop delle singole postazioni PC al fine di garantire l'assistenza tecnica e la normale attività operativa nonché la massima sicurezza contro virus, spyware, malware, etc.. L'intervento viene effettuato esclusivamente su chiamata dell'utente o, in caso di oggettiva necessità, a seguito della rilevazione tecnica di problemi nel sistema informatico e telematico o per attività di manutenzione.

3.5 Non è consentito l'uso di programmi diversi da quelli ufficialmente installati dal personale del Servizio ICT per conto dell' IISS J. VON NEUMANN né viene consentito agli utenti di installare autonomamente programmi provenienti dall'esterno, sussistendo infatti il grave pericolo di introdurre Virus informatici e/o di alterare la funzionalità delle applicazioni software esistenti. L'inosservanza della presente disposizione espone lo stesso IISS J. VON NEUMANN a gravi responsabilità civili; si evidenzia inoltre che le violazioni della normativa a tutela dei diritti d'autore sul software che impone la presenza nel sistema di software regolarmente licenziato, o comunque libero e quindi non protetto dal diritto d'autore, vengono sanzionate anche penalmente.

3.6 Salvo preventiva espressa autorizzazione del personale del Servizio ICT, non è consentito all'utente modificare le caratteristiche impostate sul proprio PC né procedere ad installare dispositivi di memorizzazione, comunicazione o altro (come ad esempio masterizzatori, modem, etc.).

3.7 Ogni utente deve prestare la massima attenzione ai supporti di origine esterna, avvertendo immediatamente il personale del Servizio ICT nel caso in cui siano rilevati virus ed adottando quanto previsto dal successivo punto 10 del presente Regolamento relativo alle procedure di protezione antivirus.

3.8 Il Personal Computer deve essere spento ogni sera prima di lasciare gli uffici o in caso di assenze prolungate dall'ufficio o in caso di suo inutilizzo. In ogni caso, 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. Al fine di evitare tali evenienze si dovrà "bloccare" l'utilizzo del PC prima di allontanarsi o impostare la modalità "screen saver" che prevede la richiesta della password per riattivarne l'uso**.**

4. Gestione ed assegnazione delle credenziali di autenticazione

4.1 Le credenziali di autenticazione per l'accesso alla rete vengono assegnate dal personale del Servizio ICT, previa formale richiesta del Responsabile dell'ufficio/area nell'ambito del quale verrà inserito ed andrà ad operare il nuovo utente. Nel caso di collaboratori a progetto e coordinati e continuativi la preventiva richiesta, se necessario, verrà inoltrata dal Titolare del trattamento.

4.2 Le credenziali di autenticazione consistono in un codice per l'identificazione dell'utente (user id), assegnato dal Servizio ICT, associato ad una parola chiave (password) riservata che dovrà

venir custodita dall'autorizzato con la massima diligenza e non divulgata. Non è consentita l'attivazione della password di accensione (bios), senza preventiva autorizzazione da parte del Servizio ICT.

4.3 La parola chiave, formata da lettere (maiuscole o minuscole) e/o numeri, anche in combinazione fra loro, deve essere composta da almeno otto caratteri e non deve contenere riferimenti agevolmente riconducibili all'autorizzato. Per costruire la password utilizzare:

- lettere, numeri e almeno un carattere tra . ; $! @ - > <
- Non utilizzare date di nascita, nomi o cognomi propri o di parenti
- Non sceglierla uguale alla matricola o alla userid
- Custodirla sempre in un luogo sicuro e non accessibile a terzi
- Non divulgarla a terzi e non condividerla con altri utenti

4.4 È necessario procedere alla modifica della parola chiave a cura dell'utente, ove ciò non avvenga grazie a processi automatici del sistema informativo, al primo utilizzo e, successivamente, almeno ogni sei mesi (Ogni tre mesi nel caso invece di trattamento di dati sensibili attraverso l'ausilio di strumenti elettronici).

4.5 Qualora la parola chiave dovesse venir sostituita, per decorso del termine sopra previsto e/o in quanto abbia perduto la propria riservatezza, si procederà in tal senso d'intesa con il personale del Servizio ICT.

5. Utilizzo della rete di

5.1 Per l'accesso alla rete dell' IISS J. VON NEUMANN ciascun utente deve essere in possesso della specifica credenziale di autenticazione.

5.2 È assolutamente proibito entrare nella rete e nei programmi con un codice d'identificazione utente diverso da quello assegnato. Le parole chiave d'ingresso alla rete ed ai programmi sono segrete e vanno comunicate e gestite secondo le istruzioni impartite.

5.3 Le cartelle utenti presenti nei server dell' IISS J. VON NEUMANN sono aree di condivisione di informazioni strettamente professionali e non possono in alcun modo essere utilizzate per scopi diversi. Pertanto, qualunque file che non sia legato all'attività lavorativa non può essere dislocato, nemmeno per brevi periodi, in queste unità. Su queste unità vengono svolte regolari attività di controllo, amministrazione e back up da parte del personale del Servizio ICT. Si ricorda che tutti i dischi o altre unità di memorizzazione locali (es. disco C: interno PC) non sono soggette a salvataggio da parte del personale autorizzato del Servizio ICT. La responsabilità del salvataggio dei dati ivi contenuti è pertanto a carico del singolo utente.

5.4 Il personale del Servizio ICT può in qualunque momento procedere alla rimozione di ogni file o applicazione che riterrà essere pericolosi per la Sicurezza sia sui PC degli incaricati sia sulle unità di rete.

5.5 Risulta opportuno che, con regolare periodicità (almeno ogni tre mesi), ciascun utente provveda alla pulizia degli archivi del proprio PC, con cancellazione dei file obsoleti o inutili. Particolare attenzione deve essere prestata alla duplicazione dei dati, essendo infatti necessario evitare un'archiviazione ridondante.

6. Utilizzo e conservazione dei supporti rimovibili

6.1 Tutti i supporti magnetici rimovibili (dischetti, CD e DVD riscrivibili, supporti USB, ecc.), contenenti dati rilevanti dal punto di vista del business (classificabili come riservati e/o confidenziali) nonché informazioni costituenti know-how ISTITUTO le, devono essere trattati con particolare cautela onde evitare che il loro contenuto possa essere trafugato o alterato e/o distrutto o, successivamente alla cancellazione, recuperato.

6.2 Al fine di assicurare la distruzione e/o inutilizzabilità di supporti magnetici rimovibili contenenti dati sensibili, ciascun utente dovrà contattare il personale del Servizio ICT e seguire le istruzioni da questo impartite.

6.3 In ogni caso, i supporti magnetici contenenti dati **particolari/sensibili**, secondo la definizione dell'art. 4 del GDPR e del Codice, devono essere adeguatamente custoditi dagli utenti e risposti in armadi chiusi ad accesso controllato.

6.4 È vietato l'utilizzo di supporti rimovibili personali.

6.5 L'utente è responsabile della custodia dei supporti e dei dati ISTITUTO li in essi contenuti.

7. Utilizzo di PC portatili personali

7.1 L'utente è responsabile del PC portatile affidato e deve custodirlo con diligenza sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro.

7.2 I PC portatili utilizzati all'esterno, in caso di allontanamento, devono essere custoditi con diligenza, adottando tutti i provvedimenti che le circostanze rendono necessari per evitare danni o sottrazioni.

8. Uso della posta elettronica

8.1 **La casella di posta elettronica assegnata all'utente è uno strumento di lavoro.** Le persone assegnatarie delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse.

8.2 È fatto divieto di utilizzare le caselle di posta elettronica ISTITUTO li per motivi diversi da quelli strettamente legati all'attività lavorativa. In questo senso, a titolo puramente esemplificativo, l'utente non potrà utilizzare la posta elettronica per:

- l'invio e/o il ricevimento di allegati contenenti filmati o brani musicali (es.mp3) non legati all'attività lavorativa;
- l'invio e/o il ricevimento di messaggi personali o per la partecipazione a dibattiti, aste on line, concorsi, forum o mailing-list;
- la partecipazione a catene telematiche (o di Sant'Antonio). Se si dovessero peraltro ricevere messaggi di tale tipo, si deve comunicarlo immediatamente al personale del Servizio ICT. Non si dovrà in alcun caso procedere all'apertura degli allegati a tali messaggi.

8.3 La casella di posta deve essere mantenuta in ordine, cancellando documenti inutili.

8.4 Ogni comunicazione inviata o ricevuta che abbia contenuti rilevanti o contenga impegni contrattuali o precontrattuali per l'IISS J. VON NEUMANN ovvero contenga documenti da considerarsi riservati in quanto contraddistinti dalla dicitura "strettamente riservati" o da analoga dicitura, deve essere preventivamente visionata od autorizzata dal Responsabile d'ufficio.

8.5 È possibile utilizzare la ricevuta di ritorno per avere la conferma dell'avvenuta lettura del messaggio da parte del destinatario. Si evidenzia però che le comunicazioni ufficiali, da inviarsi mediante gli strumenti tradizionali (fax, posta, …), possono richiedere l'autorizzazione e la firma dei Responsabili di ufficio, a seconda del loro contenuto e dei destinatari delle stesse.

8.6 È obbligatorio controllare i file attachment di posta elettronica prima del loro utilizzo (non eseguire download di file eseguibili o documenti da siti Web o Ftp non conosciuti).

8.7 Al fine di garantire la funzionalità del servizio di posta elettronica istituzionale e di ridurre al minimo l'accesso ai dati, nel rispetto del principio di necessità e di proporzionalità, il sistema, in caso di assenze (ad es. per ferie o attività di lavoro fuori sede dell'assegnatario della casella, o malattia) invierà automaticamente messaggi di risposta contenenti le "coordinate" di posta elettronica di un altro soggetto o altre utili modalità di contatto della struttura. In caso di assenze programmate la funzionalità deve essere attivata dall'utente; in caso di assenza non programmata (ad es. per malattia) verrà attivata a cura dell' IISS J. VON NEUMANN.

8.8 Al fine di ribadire agli interlocutori la natura esclusivamente ISTITUTO le della casella di posta elettronica, i messaggi devono contenere un avvertimento standardizzato nel quale sia dichiarata la natura non personale dei messaggi stessi precisando che, pertanto, personale dipendente dell'IISS J. VON NEUMANN debitamente autorizzato potrà accedere al contenuto del messaggio inviato alla stessa casella secondo le regole fissate nella propria policy. Si riportano di seguito i testi da utilizzare:

Nota di riservatezza: Il presente messaggio, corredato dei relativi allegati contiene informazioni da considerarsi strettamente riservate, ed è destinato esclusivamente al destinatario sopra indicato, il quale è l'unico autorizzato ad usarlo, copiarlo e, sotto la propria responsabilità, diffonderlo. Chiunque ricevesse questo messaggio per errore o comunque lo leggesse senza esserne legittimato è avvertito che trattenerlo, copiarlo, divulgarlo, distribuirlo a persone diverse dal destinatario è severamente proibito, ed è pregato di rinviarlo immediatamente al mittente distruggendo l'originale.

8.9 Come anticipato al precedente punto 3.3 del presente Regolamento, il personale autorizzato del Servizio ICT potrà accedere ai dati contenuti nelle caselle di posta elettronica di lavoro per le sole finalità ivi indicate.

9. Navigazione in Internet

9.1. **Il PC assegnato al singolo utente ed abilitato alla navigazione in Internet costituisce uno strumento dell' IISS J. VON NEUMANN e utilizzabile esclusivamente per lo svolgimento della propria attività lavorativa**. È quindi assolutamente proibita la navigazione in Internet per motivi diversi da quelli strettamente legati all'attività lavorativa.

10. Utilizzo Piattaforme

ARGO WEB
SIDI MIUR

11. Protezione antivirus

10.1 Il sistema informatico dell'IISS J. VON NEUMANN è protetto da software antivirus aggiornato periodicamente. Ogni utente deve comunque tenere comportamenti tali da ridurre il rischio di attacco al sistema informatico dell'IISS J. VON NEUMANN mediante virus o mediante ogni altro software aggressivo.

10.2 Nel caso il software antivirus rilevi la presenza di un virus, l'utente dovrà immediatamente sospendere ogni elaborazione in corso senza spegnere il computer nonché segnalare prontamente l'accaduto al personale assistente tecnico dell'IISS J. VON NEUMANN.

10.3 Ogni dispositivo magnetico di provenienza esterna all'IISS J. VON NEUMANN dovrà essere verificato mediante il programma antivirus prima del suo utilizzo e, nel caso venga rilevato un virus, dovrà essere prontamente consegnato al personale del Servizio ICT.

11. Utilizzo dei telefoni, fax e fotocopiatrici

11.1 Il telefono in uso all'utente è uno strumento di lavoro. Ne viene concesso l'uso esclusivamente per lo svolgimento dell'attività lavorativa, non essendo quindi consentite comunicazioni a carattere personale o comunque non strettamente inerenti all'attività lavorativa stessa. La ricezione o l'effettuazione di telefonate personali è consentita sempre che vengano rispettati i criteri di ragionevolezza ovvero nel caso di necessità ed urgenza. Si evidenzia che a fronte di volumi di traffico anomali saranno poste in essere le opportune analisi mirate a rilevare eventuali utilizzi impropri.

11.2 È vietato l'utilizzo dei fax dell'IISS J. VON NEUMANN per fini personali, tanto per spedire quanto per ricevere documentazione, salva diversa esplicita autorizzazione da parte del Responsabile di ufficio.

11.3 È vietato l'utilizzo delle fotocopiatrici dell'IISS J. VON NEUMANN per fini personali, salvo preventiva ed esplicita autorizzazione da parte del Responsabile di ufficio.

12. Osservanza delle disposizioni in materia di Privacy

12.1 È obbligatorio attenersi alle disposizioni in materia di protezione dei dati personali previste dal GDPR, e dal Codice, rispettando le misure di sicurezza adottate dall'IISS J. VON NEUMANN, nonché le istruzioni fornite con la designazione ad "autorizzato del trattamento dei dati", come previsto dall'art. 29 del GDPR, applicando puntualmente le disposizioni ivi contenute nonché ogni ulteriore indicazione comunicata, anche per le vie brevi, dal Responsabile d'ufficio.

12.2 Gli "incaricati del trattamento" che sono addetti alle attività di amministrazione e gestione dei Sistemi, Data Base e della Infrastruttura di connessione (c.d. System Admin, DB Admin e Network Admin.) dovranno rispettare le specifiche istruzioni loro fornite al fine di rispettare i

principi di necessità e di legittimità e correttezza nella effettuazione delle loro attività. I nominativi di coloro che hanno competenza sui sistemi che trattano dati personali dei dipendenti dell' IISS J. VON NEUMANN potranno essere comunicati nelle modalità e con le forme previste dalla normativa applicabile.

13. Accesso ai dati trattati dall'utente

13.1 Oltre che per motivi di sicurezza del sistema informatico, anche per motivi tecnici e/o manutentivi (ad esempio, aggiornamento/sostituzione/implementazione di programmi, manutenzione hardware, etc.) o per finalità di controllo e programmazione dei costi (ad esempio, verifica costi di connessione ad internet, traffico telefonico, etc.), comunque estranei a qualsiasi finalità di controllo dell'attività lavorativa, è facoltà dell' IISS J. VON NEUMANN, direttamente o per il tramite del personale del Servizio ICT o degli addetti alla manutenzione, accedere direttamente, nel rispetto della normativa sulla privacy, a tutti gli strumenti informatici dell' IISS J. VON NEUMANN e ai documenti ivi contenuti, nonché ai tabulati del traffico telefonico.