



LICEO GINNASIO STATALE
VITTORIO EMANUELE II

Via S. Sebastiano, 51 - 80134 Napoli - Tel. 081 459142 – Fax 081 447698

Distretto scol. 47 - Cod. mecc. NA PC16000X – C.F. 80022960639

www.liceovittorioemanuele.it – mail: info@liceovittorioemanuele.it – napc16000x@pec.istruzione.it

Prot. 3538/D4 del 2/XII/2011

Documento Programmatico sulla Sicurezza

D.Lvo 196 del 30 giugno 2003

**PIANO OPERATIVO PER L'ADOZIONE
DELLE MISURE MINIME DI SICUREZZA
NEL TRATTAMENTO DEI DATI PERSONALI
NELL'AMBITO DELLE ATTIVITÀ**

del Liceo Classico Statale *Vittorio Emanuele II*

Indice

1. PREMESSA

2. ELENCO DEI TRATTAMENTI DEI DATI PERSONALI

- 2.1 Dati trattati dai docenti
- 2.2 Dati trattati dal personale amministrativo
- 2.3 Dati trattati dai collaboratori scolastici
- 2.4 Dati trattati dagli assistenti tecnici
- 2.5 Dati trattati dal dirigente scolastico

3. DISTRIBUZIONE DEI COMPITI E DELLE RESPONSABILITÀ

3.1 Individuazione e attribuzione delle responsabilità. Individuazione dei soggetti

- 3.1.1 Il titolare
- 3.1.2 Il responsabile del trattamento dei dati
- 3.1.3 Gli incaricati
- 3.1.4 L'amministratore di sistema (rete didattica)
- 3.1.5 L'amministratore di sistema (rete di segreteria)

4. ANALISI DEI RISCHI CHE INCOMBONO SUI DATI

4.1 Il sistema informativo

- 4.1.1 Rete amministrativa
- 4.1.2 Rete didattica
- 4.1.3 Policy

4.2 Analisi del rischio

- 4.2.1 Rischio fisico
 - 4.2.1.1 Archivi cartacei
 - 4.2.1.2 Archivi informatici
 - 4.2.1.3 Misure di sicurezza relative agli accessi

4.2.2 Rischio logico

5. MISURE MINIME DI SICUREZZA ADOTTATE

5.1 Archivi su supporto cartaceo

- 5.1.1 Norme per i dati sensibili e giudiziari

5.2 Archivi su supporto informatico

5.3 Sicurezza fisica dei computer

5.4 Difesa da accessi non autorizzati da rete geografica

5.5 Codice identificativo degli utenti del sistema informativo

5.6 Password

- 5.6.1 Misure di carattere elettronico/informatico
- 5.6.2 Regole per la gestione delle password
- 5.6.3 Regole di comportamento per minimizzare i rischi da virus
- 5.6.4 *Incident response* e ripristino

5.7 Protezione degli archivi informatici contenenti dati sensibili e giudiziari

5.8 Salvataggio dei dati di backup

5.9 La cassaforte

5.10 Protezione da virus informatici

5.11 Protezione da rischi durante la trasmissione dati

5.12 Riutilizzo dei supporti di memorizzazione dei dati sensibili

6. MODALITÀ PER IL RIPRISTINO DELLA DISPONIBILITÀ DEI DATI IN SEGUITO A DISTRUZIONE E DANNEGGIAMENTO

7. FORMAZIONE

8. MISURE SPECIFICHE PER I DATI PERSONALI IDONEI A RIVELARE LO STATO DI SALUTE

ALLEGATO 1 : REGOLAMENTO PER L'UTILIZZO DELLA RETE

ALLEGATO 2 : VIDEOSORVEGLIANZA

PREMESSA

Il Liceo Classico Statale “Vittorio Emanuele II” con sede in Napoli, via S. Sebastiano n. 51, cap. 80134, nella persona del suo legale rappresentante prof. Carlo ANTONELLI ha redatto il seguente documento programmatico per la sicurezza ai sensi e per gli effetti degli artt. dal 33 al 36 del D.Lgs. n.196 del 30 giugno 2003 (se nel testo si trovano indicati solo gli articoli si fa riferimento a tale testo unico) e del “disciplinare tecnico in materie di misure minime di sicurezza” allegato al medesimo decreto.

Scopo del presente documento è quello di delineare il quadro delle misure di sicurezza, organizzative, fisiche e logiche, di seguito specificate, che saranno adottate da questa amministrazione relativamente al trattamento dei dati personali.

2. ELENCO DEI TRATTAMENTI DEI DATI PERSONALI

2.1 DATI TRATTATI DAI DOCENTI

Le banche dati cui ha accesso il singolo docente sono:

- il registro personale;
- gli elaborati degli alunni;

Le banche dati cui hanno accesso più docenti sono:

- il registro di classe;
- il registro dei verbali del consiglio di classe;
- la documentazione relativa alla programmazione didattica;
- i documenti di valutazione;
- la documentazione dello stato di handicap;
- la corrispondenza con le famiglie;
- la documentazione giustificativa delle assenze degli alunni (es. festività religiose, certificati medici, etc).

I dati trattati dai docenti sono, nel loro insieme, dati sensibili e ipersensibili, ai sensi dell’art.4 comma 1 lett. b, c, d. Il trattamento dei dati da parte dei docenti (tenuta dei registri, modalità di compilazione dei documenti di valutazione, verbalizzazione, etc.) è definito puntualmente da norme di legge o regolamentari.

2.2. DATI TRATTATI DAL PERSONALE AMMINISTRATIVO

Le banche dati su supporto cartaceo e/o informatizzato, contenenti dati personali, cui ha accesso il personale di segreteria, raggruppati in insiemi omogenei, sono:

- anagrafica e fascicoli personali degli alunni e degli ex alunni;
- registro degli infortuni;
- documentazione relativa alla gestione e adozione libri di testo;
- progetti di istituto;
- anagrafe Enti Locali;
- circolari interne;
- protocollo;
- anagrafica e fascicoli personali Docenti e ATA;
- retribuzioni Docenti e ATA;

- corrispondenza in uscita;
- graduatorie interne ed esterne;
- domande di trasferimento;

- organici;
- anagrafe fornitori;
- documentazione finanziaria e contabile;
- congedi Docenti e ATA;
- contratti e convenzioni;
- documentazione didattica trattata dai Docenti per la conservazione.

2.3. DATI TRATTATI DAI COLLABORATORI SCOLASTICI

I trattamenti che riguardano la categoria Collaboratori Scolastici consistono nello spostare, custodire, consegnare o spostare documenti contenenti dati trattati dalle altre strutture organizzative.

2.4. DATI TRATTATI DAGLI ASSISTENTI TECNICI

I trattamenti che riguardano la categoria Assistenti Tecnici consistono in tutto ciò che concerne la manipolazione, in occasione di eventuali interventi di manutenzione e riparazione, di dati sensibili eventualmente presenti nei laboratori.

2.5 DATI TRATTATI DAL DIRIGENTE SCOLASTICO

Le banche dati di pertinenza del Dirigente sono:

- i verbali delle assemblee degli Organi Collegiali;
- il protocollo riservato.

3. DISTRIBUZIONE DEI COMPITI E DELLE RESPONSABILITÀ

Il Decreto sulla protezione dei dati personali individua all'art. 4, i quattro soggetti che sono coinvolti nel trattamento dei dati personali:

- **il titolare**, cioè la persona fisica e giuridica che ha la responsabilità finale ed assume decisioni fondamentali riferite al trattamento dei dati personali;
- **il responsabile**, la persona dotata di particolari caratteristiche di natura morale e di competenza tecnica, preposta dal titolare al trattamento dei dati personali “ivi compreso il profilo della sicurezza”;
- **l'incaricato**, la persona fisica che materialmente provvede al trattamento dei dati, secondo le istruzioni impartite dal titolare o dal responsabile;
- **l'interessato**, il soggetto cui i dati oggetto di trattamento si riferiscono.

Il DPR 318/99 individuava, all'art.1, un nuovo soggetto che si aggiunge ai quattro descritti in precedenza:

- **l'amministratore di sistema informatico**, il soggetto che garantisce la tutela ed il corretto uso dei sistemi informatici e delle banche dati in esso contenuti.

Nel D.Lvo n.196/2003 non viene riproposta la figura dell'Amministratore di sistema che pur conserva una propria funzionalità per la garanzia delle misure di sicurezza logica del sistema informatico della gestione dei dati. Pertanto si ravvisa la necessità di individuare tale figura con delega di compiti definiti.

3.1 INDIVIDUAZIONE E ATTRIBUZIONE DELLE RESPONSABILITÀ, INDIVIDUAZIONE DEI SOGGETTI

3.1.1 Il Titolare

Il Titolare del trattamento è l'istituzione scolastica e la titolarità è esercitata dal **Dirigente Scolastico** (art. 28).

Tra i compiti che la legge gli assegna e che non sono delegabili, è prevista la vigilanza sul rispetto da parte del Responsabile delle proprie istruzioni, nonché sulla puntuale osservanza delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza. Il Titolare è il soggetto che assume le decisioni sulle modalità e le finalità del trattamento.

3.1.2 Il responsabile del trattamento dei dati

In base a quanto disposto dal D.Lvo n.196/2003, il Dirigente Scolastico, in qualità di Titolare del trattamento dei dati, individua come Responsabile per il trattamento dei dati personali ai fini della sicurezza il Sig. Luigi DI STADIO con il compito di:

- promuovere lo sviluppo, la realizzazione ed il mantenimento del programma di sicurezza e vigilare sul rispetto delle norme indicate nel presente Documento Programmatico sulla Sicurezza;
- informare prontamente il Titolare di ogni questione rilevante ai fini della legge;
- operare perché il trattamento dei dati avvenga secondo le modalità definite dalla normativa in vigore;
- verificare che il trattamento dei dati avvenga in modo lecito;
- verificare che l'informativa all'interessato sia stata effettuata;
- operare per garantire l'effettivo esercizio dei diritti dell'interessato;
- rispettare e far rispettare le misure di sicurezza indicate dalla vigente normativa in materia di tutela dei dati personali e predisposte da questa istituzione scolastica, nel proprio ambito di competenza;
- provvedere alla gestione delle chiavi degli archivi che contengono dati personali;
- verificare che vi sia il consenso dell'interessato per il trattamento dei dati sensibili, se necessario;
- promuovere lo svolgimento di un continuo programma di addestramento degli incaricati del trattamento e mantenere attivo un programma di controllo e monitoraggio della corrispondenza con le regole di sicurezza.

3.1.3 Gli incaricati

Il Titolare del trattamento dei dati individua gli incaricati in relazione alle operazioni di elaborazione di dati personali ai quali i soggetti hanno accesso nell'espletamento della loro funzione e/o per gli incarichi che sono loro affidati.

In ottemperanza al Decreto che regola il trattamento dei dati personali, laddove costituisce trattamento "qualunque operazione o complesso di operazioni svolte con o senza l'ausilio di mezzi elettronici o comunque automatizzati, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distribuzione dei dati", l'incaricato deve trattare i dati personali:

1. in modo lecito e secondo correttezza;
2. raccogliendoli e registrandoli per gli scopi inerenti l'attività svolta;
3. verificando, ove possibile, che siano esatti e, se necessario, aggiornandoli;
4. verificando che siano pertinenti, completi e non eccedenti le finalità per le quali sono stati raccolti o successivamente trattati, secondo le indicazioni ricevute dal Responsabile/Titolare;

5. rispettando, nella conservazione, le misure di sicurezza predisposte nell'istituzione;
6. effettuando le seguenti operazioni nel trattamento dei documenti (documentazione didattica contenente dati personali):
 - non far uscire documenti dalla sede scolastica, neanche temporaneamente;
 - non fare copie della documentazione, salvo autorizzazione del responsabile o del titolare;
 - durante il trattamento mantenere i documenti contenenti dati personali non alla portata di vista di terzi;
 - al termine del trattamento custodire i documenti all'interno di archivi muniti di serratura;
 - in caso di allontanamento anche temporaneo dal posto di lavoro, o comunque dal luogo dove vengono trattati i dati, l'incaricato dovrà verificare che non vi sia possibilità da parte di terzi, anche se dipendenti non incaricati, di accedere a dati personali per i quali era in corso un qualunque tipo di trattamento.
7. nessun dato potrà essere comunicato a terzi o diffuso senza la preventiva specifica autorizzazione del Titolare o Responsabile;
8. le comunicazioni agli interessati (genitori o chi ne fa le veci) dovranno avvenire in forma riservata, se effettuate per scritto dovranno essere consegnate in contenitori chiusi;
9. all'atto della consegna di documenti l'incaricato dovrà assicurarsi dell'identità dell'interessato o di chi è stato delegato al ritiro del documento in forma scritta.

Gli incaricati del trattamento dei dati personali, con specifico riferimento alla sicurezza, hanno le seguenti responsabilità:

- svolgere le attività previste dai trattamenti secondo le prescrizioni contenute nel presente Documento Programmatico sulla Sicurezza e le direttive del Responsabile del trattamento dei dati;
- non modificare i trattamenti esistenti o introdurre nuovi trattamenti senza l'esplicita autorizzazione del Responsabile del trattamento dei dati;
- rispettare e far rispettare le norme di sicurezza per la protezione dei dati personali;
- informare il Responsabile in caso di incidente di sicurezza che coinvolga dati sensibili e non.

Il **docente** è da considerarsi, per la propria sfera di competenza, incaricato del trattamento dei dati e come tale è nominato mediante specifico atto di designazione. Tale nomina elenca puntualmente: categorie dei dati cui può avere accesso, tipologia di trattamento e vincoli specifici applicabili alla varie tipologie di dati, istruzioni in merito ai soggetti cui i dati possono essere comunicati o diffusi.

Il **D.S.G.A.**, il **responsabile dell'ufficio tecnico** e ogni **assistente amministrativo** è nominato incaricato del trattamento con specifico atto di designazione, in base ai compiti che assolve nell'ufficio. Tale nomina elenca puntualmente: categorie dei dati cui può avere accesso, tipologia di trattamento e vincoli specifici applicabili alla varie tipologie di dati, istruzioni in merito ai soggetti cui i dati possono essere comunicati o diffusi.

I **collaboratori scolastici**, e gli **assistenti tecnici** poichè trattano, anche se saltuariamente, dati personali, sono nominati incaricati con specifico atto di designazione. Tale nomina elenca puntualmente: categorie dei dati cui può avere accesso, tipologia di trattamento e vincoli specifici applicabili alla varie tipologie di dati, istruzioni in merito ai soggetti cui i dati possono essere comunicati o diffusi.

Le nomine saranno effettuate anche per il personale supplente temporaneo, docente e ATA, e, per quanto riguarda i trattamenti effettuati con strumenti elettronici, per il personale esterno eventualmente incaricato della manutenzione.

3.1.4 L'amministratore di sistema rete amministrativa

L'amministratore di sistema rete amministrativa ha l'incarico di:

- sovrintendere al funzionamento della rete, compresa la protezione da virus informatici;
- monitorare lo stato dei sistemi, con particolare attenzione alla sicurezza;
- effettuare interventi di manutenzione hardware e software su sistemi operativi e applicativi, compresa la gestione e la configurazione della posta elettronica e la gestione degli ambienti riservati di comunicazione e trasmissione dati tra la scuola e gli altri enti pubblici (MEF, INPS, INPDAP, MIUR, CSA, Provincia, Regione....);
- fare in modo che sia prevista la disattivazione dei codici identificativi personali (user-id), in caso di perdita della qualità che consentiva all'incaricato l'accesso al personal computer, oppure nel caso di mancato utilizzo del codice per oltre sei mesi;
- collaborare con il responsabile del trattamento dei dati personali;
- informare tempestivamente il responsabile del trattamento dei dati sulle non corrispondenze con le norme di sicurezza, su eventuali incidenti e variazioni di ogni tipo.

3.1.5 L'amministratore di sistema rete di Istituto ad esclusione della rete amministrativa

L'amministratore di sistema rete di Istituto ad esclusione della rete amministrativa ha l'incarico di:

- sovrintendere al funzionamento della rete, comprese le apparecchiature di protezione
- (firewall, filtri);
- monitorare lo stato dei sistemi, con particolare attenzione alla sicurezza;
- effettuare interventi di manutenzione hardware e software su sistemi operativi e applicativi;
- fare in modo che sia prevista la disattivazione dei codici identificativi personali (user-id), in caso di perdita della qualità che consentiva all'incaricato l'accesso al personal computer, oppure nel caso di mancato utilizzo del codice per oltre sei mesi;
- collaborare con il responsabile del trattamento dei dati personali;
- informare tempestivamente il responsabile del trattamento dei dati sulle non corrispondenze con le norme di sicurezza, su eventuali incidenti e variazioni di ogni tipo.

4. ANALISI DEI RISCHI CHE INCOMBONO SUI DATI

4.1 IL SISTEMA INFORMATIVO

Il Sistema Informativo del Liceo "Vittorio Emanuele II" è formato: n. 1 rete amministrativa costituita da n. 8 postazioni di personal computer Intel Pentium di varie potenze e capacità elaborative con sistemi operativi Windows XP, Vista, alla quale fanno parte tutte le unità di segreteria e un punto di connessione (solo dal punto di vista della connettività) inerente i laboratori di Chimica e di Fisica; n. 1 rete didattica che riunisce i due laboratori (informatica e linguistico-multimediale), il Pc del D.S, i computer in uso dei docenti collaboratori del Dirigente in vicepresidenza, il computer nella Sala Professori e in Biblioteca.

4.1.1 Rete amministrativa

Tutti i posti di lavoro sono connessi in rete locale mediante switch di dominio e cablaggio Ethernet UTP RJ45 con protocollo TCP/IP.

N. 8 personal computer sono riservati all'amministrazione (n. 6 situati nei locali della segreteria e n. 2 nell'ufficio del DSGA).

Il server, compreso nel numero di cui sopra, si trova in una delle stanze adibita a segreteria amministrativa. La segreteria è, a sua volta, protetta da porta e grate di ferro alle finestre.

Tutti i computer sono dotati di indirizzo IP dinamico assegnato dal DHCP.

La connettività internet avviene attraverso Router con indirizzo IP statico.

4.1.2 Rete didattica

Tutti i posti di lavoro sono connessi in rete locale mediante switch e cablaggio Ethernet UTP RJ45 con protocollo TCP/IP, i computer sono localizzati nei laboratori, nella zona presidenza, vicepresidenza, sala docenti e biblioteca.

Il server si trova nella presidenza protetta da porta e grate di ferro alla finestra.

Tutti i computer sono dotati di indirizzo IP statico assegnato dall'amministratore.

La connettività a internet avviene attraverso Router con indirizzo IP statico gestito con sistema operativo Linux.

4.1.3 Policy

Tutti gli utenti della rete devono rispettare le norme previste nel documento policy di utilizzo della rete.

Il server della rete amministrativa (windows XP) si trova nel locale della segreteria come già detto sopra.

Il server della rete didattica si trova nell'ufficio di presidenza.

4.2 ANALISI DEL RISCHIO

I rischi a cui sono sottoposti gli archivi presenti nella scuola si possono suddividere in rischi **fisici** e **logici**.

Alla prima tipologia appartengono tutti gli archivi a supporto cartaceo e in parte quelli su supporto informatico. Alla seconda tipologia appartengono quelli che utilizzano elaboratori elettronici ed in specie quelli connessi in rete, sia locale che geografica.

4.2.1 Rischio fisico

Il furto o il danneggiamento degli archivi, la diffusione o distruzione non autorizzata di informazioni personali e l'interruzione dei processi informatici possono esporre il Liceo Classico Statale "Vittorio Emanuele II" al rischio di violazione di legge.

4.2.1.1 Archivi cartacei

Gli archivi cartacei sono conservati in armadi nei locali della segreteria, dotati di porta con chiave e in un archivio chiuso con porta blindata.

I rischi fisici a cui sono sottoposti sono i seguenti:

1. accesso agli uffici e agli archivi di persone esterne alla Scuola;
2. smarrimento per incuria da parte del personale;
3. furto;
4. visura e/o copiatura da parte di personale non autorizzato;
5. perdita parziale o totale a causa di incendi o allagamenti;
6. perdita parziale o totale per il degrado naturale del supporto (invecchiamento);
7. atti di vandalismo.

4.2.1.2 Archivi informatici

Gli archivi informatizzati risiedono su elaboratori elettronici. I rischi fisici a cui sono soggetti sono i seguenti:

1. distruzione fisica dell'elaboratore per eventi esterni allo stesso quali, incendi, allagamenti, sbalzi di corrente;
2. guasti hardware dell'elaboratore tali da impedire il recupero degli archivi che si trovano sugli hard disk;
3. furto dell'elaboratore e/o dei supporti di backup dei dati;
4. perdita di dati dovuta a imperizia del personale addetto;
5. accesso agli elaboratori da parte di personale non autorizzato;
6. interruzione dei servizi di connessione fisica alla rete (linee telefoniche, router, modem, switch, hub);
7. atti di vandalismo.

4.2.1.3 Misure di sicurezza relative agli accessi fisici

Sono definite aree ad accesso controllato quei locali che contengono apparecchiature informatiche critiche (server di rete, computer utilizzati per il trattamento dei dati sensibili e apparecchiature di telecomunicazione) e archivi informatici e/o cartacei contenenti dati sensibili; tali aree devono essere all'interno di locali sotto la responsabilità del Liceo Classico Statale "Vittorio Emanuele II". Il locale deve poter essere chiuso con chiave e l'accesso deve essere consentito solo alle persone autorizzate.

4.2.2 Rischio logico

Il rischio logico si riferisce all'utilizzo di elaboratori per la gestione degli archivi sia di dati comuni che sensibili. I rischi di questo tipo si possono così sintetizzare:

1. rischio interno all'organizzazione relativo all'utilizzo della LAN/Intranet ;
2. accesso alle banche dati da parte di personale esterno alla Scuola;
3. accesso alle informazioni da parte di personale non autorizzato attraverso i punti di contatto con il mondo esterno (Internet);
4. rischio esterno dovuto ad intrusioni nel sistema da parte di hacker;
5. rischio interno/esterno di scaricamento virus e/o trojan per mezzo di posta elettronica e/o operazioni di download eseguite tramite il browser;
6. rischio interno dovuto a intrusioni da parte di persone dell'istituto non autorizzate.

5. MISURE MINIME DI SICUREZZA ADOTTATE

Le misure minime di sicurezza adottate dal Liceo Classico Statale "Vittorio Emanuele II" si possono suddividere in due categorie:

1. destinate ai supporti cartacei;
2. destinate ai dati trattati in maniera informatica.

5.1 Archivi su supporto cartaceo

Le misure minime di sicurezza adottate per questo tipo di archivi sono così riassumibili:

- a) individuazione di tutti gli incaricati del trattamento delle informazioni;
- b) accesso ai soli dati strettamente necessari allo svolgimento delle proprie mansioni;
- c) utilizzo di archivi con accesso selezionato;

d) restituzione di atti e documenti al termine delle operazioni.

5.1.1 Norme per i dati sensibili e giudiziari

Utilizzo di armadi con controllo degli accessi agli archivi da parte del responsabile del trattamento dati.

5.2 Archivi su supporto informatico

Le misure minime di sicurezza adottate per questo tipo di archivi si riferiscono a dati sensibili e non. Si ritiene che le misure adottate, molte delle quali in uso da anni, tendano a dare la massima copertura sui rischi a prescindere dalla tipologia dei dati.

5.3 Sicurezza fisica dei computer

Il Server amministrativo (amministrazione e didattica) è situato in un ufficio di segreteria con tutte le caratteristiche segnalate sopra. La gestione è curata dalla Ditta Argo. In locale sono presenti su server i programmi alunni, personale e stipendi: gli archivi ad esso relativi sono su server remoto gestiti direttamente da Argo. Il programma relativo al Bilancio è gestito direttamente via Web quindi il programma è di carattere cloud computing, gestito sempre dalla società Argo.

Il server della rete didattica si trova nell'ufficio di presidenza

Tali apparecchiature sono accessibili solo dal personale addetto.

5.4 Difesa da accessi non autorizzati da rete geografica

La connettività Internet è fornita tramite la rete pubblica ed è protetta da appositi filtri e FIREWALL per evitare l'accesso alla rete da parte di utenti esterni non autorizzati.

5.5 Codice identificativo degli utenti del sistema informativo

Tutti gli utenti del software di segreteria Argo accedono al sistema informativo per mezzo di password personale. La password iniziale è assegnata, in collaborazione con il responsabile del sistema informativo, in maniera univoca dal responsabile per il trattamento, che assegna inoltre le aree di competenza (p.es. alunni, bilancio, stipendi) e i diritti (lettura, scrittura). User-id e password sono strettamente personali e non possono essere riassegnate ad altri utenti. La password è composta da almeno 6 caratteri.

Le password degli amministratori di sistema di tutti i server sono inserite e modificate periodicamente dai responsabili del sistema informativo; sono conservate in busta chiusa nella cassaforte.

La password di root in caso di manutenzione straordinaria può essere affidata dal responsabile del sistema informativo al sistemista addetto alla manutenzione. In tal caso essa deve essere prontamente sostituita dal responsabile al termine delle operazioni di manutenzione a cui lo stesso deve sovrintendere.

5.6 Password

La password è un elemento fondamentale per la sicurezza delle informazioni. La robustezza delle password è il meccanismo più importante per proteggere i dati; un corretto utilizzo della password è a garanzia dell'utente.

Le regole di seguito elencate sono vincolanti per tutte le postazioni tramite i quali si può accedere alla rete e alle banche dati contenenti dati sensibili.

Le password assegnate inizialmente e quelle di default dei sistemi operativi, prodotti software, ecc. devono essere immediatamente cambiate dopo l'installazione e al primo utilizzo.

Devono essere rispettate, per la definizione/gestione delle password, le regole di cui al punto 5.6.2 e, in particolare:

1. la lunghezza minima della password è di 8 caratteri;
2. non deve essere simile alla password precedente;
3. non deve contenere l'user-id come parte della password;
4. deve essere cambiata con cadenza trimestrale

In cassaforte è conservato l'archivio degli user id e delle password.

5.6.1 Misure di carattere elettronico/informatico

Le misure di carattere elettronico/informatico¹ adottate sono:

- presenza di gruppi di continuità elettrica per il server;
- attivazione di un sistema di backup centralizzato con periodicità quotidiana e storico di un mese;
- installazione di un firewall con hardware dedicato per proteggere la rete dagli accessi indesiderati attraverso internet;
- definizione delle regole per la gestione delle password per i sistemi dotati di sistemi operativi Windows XP, di seguito specificate;
- installazione di un sistema antivirus su tutti le postazioni di lavoro, configurato per controllare la posta in ingresso, la posta in uscita, per eseguire la procedura di aggiornamento in automatico con frequenza settimanale e la scansione periodica dei supporti di memoria;
- definizione delle regole per la gestione di strumenti elettronico/informatico, di seguito riportate;
- definizione delle regole di comportamento per minimizzare i rischi da virus, di seguito riportate.

5.6.2 Regole per la gestione delle password²

Tutti gli incaricati del trattamento dei dati personali accedono al sistema informativo per mezzo di un codice identificativo personale (in seguito indicato user-id) e password personale.

User-id e password iniziali sono assegnati, dal custode delle password.

User-id e password sono strettamente personali e non possono essere riassegnate ad altri utenti.

L'user-id è costituita da 8 caratteri che corrispondono alle prime otto lettere del cognome ed eventualmente del nome. In caso di omonimia si procede con le successive lettere del nome.

La password è composta da 8 caratteri alfanumerici. Detta password non contiene, né conterrà, elementi facilmente ricollegabili all'organizzazione o alla persona del suo utilizzatore e deve essere autonomamente modificata dall'incaricato al primo accesso al sistema e dallo stesso consegnata in una busta chiusa al custode delle password, il quale provvede a metterla nella cassaforte in un plico sigillato.

Ogni sei mesi (tre nel caso di trattamento dati sensibili) ciascun incaricato provvede a sostituire la propria password e a consegnare al custode delle password una busta chiusa sulla quale è indicato il proprio user-id e al cui interno è contenuta la nuova password; il custode delle password provvederà a sostituire la precedente busta con quest'ultima.

¹ Le misure di carattere elettronico/informatico sono quelle in grado di segnalare gli accessi agli elaboratori, agli applicativi, ai dati e alla rete, di gestire le copie di salvataggio dei dati e degli applicativi, di assicurare l'integrità dei dati, di proteggere gli elaboratori da programmi volutamente o involontariamente ritenuti dannosi.

² La password è un elemento fondamentale per la sicurezza delle informazioni. La robustezza delle password è il meccanismo più importante per proteggere i dati; un corretto utilizzo della password è a garanzia dell'utente.

Le password verranno automaticamente disattivate dopo tre mesi di non utilizzo.

Le password di amministratore di tutti i PC che lo prevedono sono assegnate dall'amministratore di sistema, esse sono conservate in busta chiusa nella cassaforte. In caso di necessità l'amministratore di sistema è autorizzato a intervenire sui personal computer.

In caso di manutenzione straordinaria possono essere comunicate, qualora necessario, dall'amministratore di sistema al tecnico/sistemista addetto alla manutenzione le credenziali di autenticazione di servizio. Al termine delle operazioni di manutenzione l'amministratore di sistema deve ripristinare nuove credenziali di autenticazione che devono essere custodite in cassaforte.

Le disposizioni di seguito elencate sono vincolanti per tutte le postazioni tramite i quali si può accedere alla rete e alle banche dati contenenti dati personali e/o sensibili:

- le password assegnate inizialmente e quelle di default dei sistemi operativi, prodotti software, ecc. devono essere immediatamente cambiate dopo l'installazione e al primo utilizzo;
- per la definizione/gestione della password devono essere rispettate le seguenti regole:
 - la password deve essere costituita da una sequenza di minimo otto caratteri alfanumerici e non deve essere facilmente individuabile;
 - deve contenere almeno un carattere alfabetico ed uno numerico;
 - non deve contenere più di due caratteri identici consecutivi;
 - non deve contenere lo user-id come parte della password;
 - al primo accesso la password ottenuta dal custode delle password deve essere cambiata; la nuova password non deve essere simile alla password precedente;
 - la password deve essere cambiata almeno ogni sei mesi, tre nel caso le credenziali consentano l'accesso ai dati sensibili o giudiziari;
 - la password è segreta e non deve essere comunicata ad altri;
 - la password va custodita con diligenza e riservatezza;
 - l'utente deve sostituire la password, nel caso ne accertasse la perdita o ne verificasse una rivelazione surrettizia.

5.6.3 Regole di comportamento per minimizzare i rischi da virus

Per minimizzare il rischio da virus informatici, gli utilizzatori dei PC adottano le seguenti regole:

- divieto di lavorare con diritti di amministratore o superutente sui sistemi operativi che supportano la multiutenza;
- limitare lo scambio fra computer di supporti rimovibili (floppy, cd, zip) contenenti file con estensione EXE, COM, OVR, OVL, SYS, DOC, XLS;
- controllare (scansionare con un antivirus aggiornato) qualsiasi supporto di provenienza sospetta prima di operare su uno qualsiasi dei file in esso contenuti;
- evitare l'uso di programmi shareware e di pubblico dominio se non se ne conosce la provenienza, ovvero divieto di "scaricare" dalla rete internet ogni sorta di file, eseguibile e non. La decisione di "scaricare" può essere presa solo dal responsabile del trattamento;
- disattivare gli ActiveX e il download dei file per gli utenti del browser Internet Explorer;
- disattivare la creazione di nuove finestre ed il loro ridimensionamento e impostare il livello di protezione su "chiedi conferma" (il browser avvisa quando uno script cerca di eseguire qualche azione);
- attivare la protezione massima per gli utenti del programma di posta Outlook Express al fine di proteggersi dal codice html di certi messaggi e-mail (buona norma è visualizzare e trasmettere messaggi in formato testo poiché alcune pagine web, per il solo fatto di essere visualizzate possono infettare il computer);
- non aprire gli allegati di posta se non si è certi della loro provenienza, e in ogni caso analizzarli con un software antivirus. Usare prudenza anche se un messaggio proviene da un indirizzo conosciuto (alcuni virus prendono gli indirizzi dalle mailing list e della rubrica di un computer infettato per inviare nuovi messaggi "infetti");

- non cliccare mai un link presente in un messaggio di posta elettronica da provenienza sconosciuta,(in quanto potrebbe essere falso e portare a un sito-truffa);
- non utilizzare le chat;
- consultare con periodicità settimanale la sezione sicurezza del fornitore del sistema operativo e applicare le patch di sicurezza consigliate;
- non attivare le condivisioni dell'HD in scrittura.
- seguire scrupolosamente le istruzioni fornite dal sistema antivirus nel caso in cui tale sistema antivirus abbia scoperto tempestivamente il virus (in alcuni casi esso è in grado di risolvere il problema, in altri chiederà di eliminare o cancellare il file infetto);
- avvisare l'Amministratore di sistema nel caso in cui il virus sia stato scoperto solo dopo aver subito svariati malfunzionamenti della rete o di qualche PC, ovvero in ritardo (in questo caso è possibile che l'infezione abbia raggiunto parti vitali del sistema);
- conservare i dischi di ripristino del proprio PC (creati con l'installazione del sistema operativo, o forniti direttamente dal costruttore del PC);
- conservare le copie originali di tutti i programmi applicativi utilizzati e la copia di backup consentita per legge;
- conservare la copia originale del sistema operativo e la copia di backup consentita per legge;

Nel caso di sistemi danneggiati seriamente da virus l'Amministratore procede a reinstallare il sistema operativo, i programmi applicativi ed i dati; seguendo la procedura indicata:

1. formattare l'Hard Disk, definire le partizioni e reinstallate il Sistema Operativo. (molti produttori di personal computer forniscono uno o più cd di ripristino che facilitano l'operazione);
2. installare il software antivirus, verificate e installare immediatamente gli eventuali ultimi aggiornamenti;
3. reinstallare i programmi applicativi a partire dai supporti originali;
4. effettuare il RESTORE dei soli dati a partire da una copia di backup recente. **NESSUN PROGRAMMA ESEGUIBILE DEVE ESSERE RIPRISTINATO DALLA COPIA DI BACKUP: potrebbe essere infetto;**
5. effettuare una scansione per rilevare la presenza di virus nelle copie dei dati;
6. ricordare all'utente di prestare particolare attenzione al manifestarsi di nuovi malfunzionamenti nel riprendere il lavoro di routine.

5.6.4 Incident response e ripristino³

Tutti gli incaricati del trattamento dei dati devono avvisare tempestivamente il responsabile della sicurezza informatica o l'amministratore di sistema o il responsabile del trattamento dei dati, nel caso in cui constatino le seguenti anomalie:

- discrepanze nell'uso degli user-id;
- modifica e sparizione di dati;
- cattive prestazioni del sistema (così come percepite dagli utenti);
- irregolarità nell'andamento del traffico;
- irregolarità nei tempi di utilizzo del sistema;
- quote particolarmente elevate di tentativi di connessione falliti.

In caso di incidente sono considerate le seguenti priorità:

1. evitare danni diretti alle persone;

³ Un incidente può essere definito come un evento che produce effetti negativi sulle operazioni del sistema e che si configura come frode, danno, abuso, compromissione dell'informazione, perdita di beni.

2. proteggere l'informazione sensibile o proprietaria;
3. evitare danni economici;
4. limitare i danni all'immagine dell'organizzazione.

Garantita l'incolumità fisica alle persone si procedere a:

1. isolare l'area contenente il sistema oggetto dell'incidente;
2. isolare il sistema compromesso dalla rete;
3. spegnere correttamente il sistema oggetto dell'incidente. **Una volta spento il sistema oggetto dell'incidente non deve più essere riaccesso⁴**;
4. documentare tutte le operazioni.

5.7 Protezione degli archivi informatici contenenti dati sensibili e giudiziari

Gli elaboratori che ospitano archivi con dati sensibili devono sottostare alle seguenti regole:

1. obbligo di password di BIOS;
2. autorizzazione scritta per l'accesso agli incaricati ed agli addetti alla manutenzione;
3. gli hard disk non devono essere condivisi in rete;
4. supervisione dell'incaricato del trattamento a tutte le operazioni di manutenzione;
5. antivirus costantemente aggiornato;
6. backup proceduralizzato concordato con i responsabili del trattamento e del sistema informativo;
7. conservazione in cassaforte delle copie di backup;
8. periodica formattazione dell'HD rimovibile su cui sono backappati i dati;
9. obbligo di uso di screen saver con password;
10. divieto di installazione, sui PC, di archivi con dati sensibili di carattere personale dell'utente;
11. divieto di installazione di software di qualsiasi tipo sui personal computer che contengono archivi con dati sensibili senza apposita autorizzazione scritta da parte del responsabile del trattamento dati;
12. divieto di installazione sui personal computer che contengono archivi con dati sensibili accessi remoti di qualsiasi tipo mediante modem e linee telefoniche.

Il controllo dei documenti stampati è responsabilità degli incaricati al trattamento.

La stampa di documenti contenenti dati sensibili deve essere effettuata su stampanti poste in locali ad accesso controllato o presidiate dall'incaricato.

5.8 Salvataggio dei dati di backup

Tutti gli utenti del sistema informativo sono responsabili delle operazioni di salvataggio dei propri dati. Al responsabile del trattamento dei dati compete la verifica delle operazioni connesse al salvataggio quotidiano dei dati del DB ARGO e tutte le operazioni di Restore

5.9 Cassaforte

Nei locali della scuola si trova la cassaforte, in essa sono custodite, oltre ad altri documenti le copie delle password e degli user id.

L'ubicazione della chiave della cassaforte è a conoscenza del Dirigente Scolastico, del DSGA, del responsabile delle password, e dei loro delegati.

⁴ È indispensabile che per una eventuale indagine venga assicurata l'integrità e la sicurezza dello stato del sistema in oggetto e quindi non venga introdotta alcuna alterazione ai dati residenti nel sistema medesimo; un ripristino affrettato del sistema potrebbe alterare le prove dell'incidente.

5.10 Protezione da virus informatici

Su tutti i personal computer degli utenti e sui server è installato apposito software antivirus **Kaspersky** e **Avast** in grado di prevenire attacchi di virus informatici. Detto software controlla anche le caselle di posta elettronica ed i file di attach. L'aggiornamento del software antivirus viene effettuato in modo automatico attraverso internet.

L'utilizzo di software antivirus non è sufficiente da solo a garantire e prevenire attacchi di questo tipo.

Secondo l'esperienza comune, un virus è riconducibile a un codice eseguibile in grado di generare copie di se stesso e di introdursi in file di dati e nel codice di altri programmi.

L'introduzione di un virus può essere causata da un'operazione diretta, quale il trasferimento di un file, la lettura di un e-mail, l'installazione di una applicazione da un supporto esterno (CD, USB pen-drive, HD rimovibile) o attraverso internet, o con un'azione indiretta tra cui l'apertura di un file in formato Word o Excel, contenente una macro, o la visualizzazione di una pagina Web, contenente un applet o un componente Activex.

La raccomandazione è quella di lavorare, in particolare quando si è connessi ad internet (navigare, scaricare email ecc.), come utente generico, in questo modo eventuali danni provocati da virus saranno limitati ai file a cui l'utente ha il permesso di accesso; lavorare invece come utente privilegiato, ovvero come root, abbassa il livello di sicurezza intrinseca del sistema e permette, potenzialmente, ai virus di causare seri danni.

5.11 Protezione dai rischi durante la trasmissione dati

L'eventuale trasmissione di dati ad altre amministrazioni, quali Comuni, Provincia, Regione, MEF, INPS, INPDAP, MIUR, UAT, Istituto Cassiere, può avvenire solamente sulla rete amministrativa che garantisce criteri di riservatezza e confidenzialità.

È vietato l'utilizzo di sniffer sulle reti del Liceo. L'uso di questo tipo di software è riservato esclusivamente al responsabile del sistema informativo, per la misura/diagnostica delle prestazioni di rete. Non è ammessa in ogni caso la lettura in chiaro dei pacchetti in transito. Tale operazione deve essere autorizzata dalla Autorità Giudiziaria.

5.12 Riutilizzazione dei supporti di memorizzazione di dati sensibili

I supporti di memorizzazione di dati sensibili (CD-ROM, USB pen-drive, HD rimovibili) sono soggetti alle seguenti misure di sicurezza:

1. i CD-ROM non più utilizzati devono essere distrutti fisicamente mediante rottura delle parti principali e taglio delle superfici magnetiche alla presenza dell'incaricato del trattamento;
2. gli hard disk non più utilizzabili devono essere distrutti meccanicamente alla presenza dell'incaricato del trattamento;
3. le USB pen-drive e gli hard disk ancora idonei all'uso, (come nel caso di sostituzioni o dismissioni di personal computer), devono essere formattati a basso livello alla presenza dell'incaricato del trattamento che deve accertare la reale cancellazione di tutti i dati con la collaborazione dell'Amministratore di Sistema.

6. MODALITÀ PER IL RIPRISTINO DELLA DISPONIBILITÀ DEI DATI IN SEGUITO A DISTRUZIONE E DANNEGGIAMENTO.

Il Responsabile, nel caso del verificarsi di eventi che provochino la distruzione o il danneggiamento dei dati personali contenuti nelle banche dati del sistema informatico, provvederà senza ritardo a ripristinare le funzionalità delle banche dati utilizzando le copie di back-up. (Vedi qui 5.6.4)

7. INTERVENTI FORMATIVI

Il buon funzionamento di un piano di sicurezza si realizza attraverso il coinvolgimento di tutto il personale della scuola, creando la cultura necessaria a garantire e a preservare l'integrità e la riservatezza dell'intero patrimonio informatico, con particolare attenzione ai dati sensibili.

La formazione è programmata già al momento dell'ingresso in servizio, nonché in occasione di cambiamenti di mansioni o di introduzione di nuovi significativi strumenti, rilevanti rispetto al trattamento di dati personali.

La formazione continua, che deve coinvolgere tutto il personale della scuola, deve prevedere i seguenti punti:

una analisi dettagliata ed aggiornata delle vigenti disposizioni di legge, con riferimenti anche alle normative europee (destinatari tutti);

disposizioni legislative in tema di tutela dei dati e criminalità informatico (destinatari tutti);

analisi dettagliata del D. Lvo 196/03 (destinatari tutti);

analisi e spiegazione dei ruoli: titolare, responsabile, incaricato, amministratore di sistema ecc.. (destinatari tutti);

illustrazione del presente piano (destinatari tutti);

uso consapevole della rete didattica (destinatari docenti);

uso consapevole della rete di segreteria (destinatari assistenti amministrativi);

destinazione di almeno il 20% del tempo di formazione nel settore informatica (corsi interni) ai temi della sicurezza e salvaguardia del patrimonio della scuola (antivirus, backup, accessi controllati ecc...);

sensibilizzazione degli incaricati sulle tematiche di sicurezza, in particolar modo sui rischi e sulle responsabilità che riguardano il trattamento dei dati personali;

Il piano prevede inoltre la pubblicazione di normativa ed ordini di servizio via e-mail e in appositi registri.

8. MISURE SPECIFICHE PER I DATI PERSONALI IDONEI A RIVELARE LO STATO DI SALUTE

Questa istituzione tratta dati idonei a rivelare lo stato di salute del personale, docente ed ATA, e degli alunni esclusivamente per finalità previste dalla legge.

Secondo quanto prescritto dall'art.22 comma 7 del D.Lvo n.196/2003; i dati idonei a rivelare lo stato di salute *“sono conservati separatamente da altri dati personali trattati per finalità che non richiedono il loro utilizzo”*; inoltre il comma 7 dello stesso articolo dispone che i dati idonei a rivelare lo stato di salute, qualora contenuti in banche dati informatiche, vengano trattati *“con tecniche di cifratura o mediante l'utilizzo di codici identificativi o di altre soluzioni, che li rendono temporaneamente inintelligibili anche a chi è autorizzato ad accedervi e permettono di identificare gli interessati solo in caso di necessità”*.

Riguardo al trattamento senza l'ausilio di strumenti elettronici, dei dati di cui si tratta, si stabilisce quanto segue:

Dati riguardanti il personale docente ed ATA

I dati consistono essenzialmente in certificati medici consegnati o fatti pervenire all'ufficio di segreteria.

Dopo la ricezione, verranno inseriti nel fascicolo personale, dove saranno conservati all'interno di una busta chiusa recante l'indicazione del contenuto separatamente dagli altri documenti.

Dati riguardanti gli alunni.

I dati consistono essenzialmente in certificati medici consegnati dagli alunni o dai genitori ai docenti o al personale ATA, per scopi definiti da norme di legge (giustificazione assenze, esonero da attività di educazione fisica, necessità di particolari diete alimentari, etc.).

Dopo la ricezione, verranno inseriti nel fascicolo personale, dove saranno conservati all'interno di una busta chiusa recante l'indicazione del contenuto separatamente dagli altri documenti.

Il presente Documento Programmatico sulla Sicurezza è redatto in due copie originali di cui una è conservata in cassaforte.

Il Titolare del Trattamento
(D.S. prof. Carlo Antonelli)



ALLEGATO 1 - Regolamento per l'utilizzo della rete

Articolo 1 OGGETTO E AMBITO DI APPLICAZIONE

Il presente regolamento disciplina le modalità di accesso e di uso della rete informatica e telematica del Liceo Classico Statale *Vittorio Emanuele II* (di seguito Liceo Vittorio Emanuele) e dei servizi che, tramite la stessa rete, è possibile ricevere o offrire.

La rete del Liceo Vittorio Emanuele è connessa alla rete Internet.

Articolo 2 PRINCIPI GENERALI – DIRITTI E RESPONSABILITÀ

Il Liceo Vittorio Emanuele promuove l'utilizzo della rete quale strumento utile per perseguire le proprie finalità.

Gli utenti manifestano liberamente il proprio pensiero nel rispetto dei diritti degli altri utenti e di terzi, nel rispetto dell'integrità dei sistemi e delle relative risorse fisiche, in osservanza delle leggi, norme e obblighi contrattuali.

Consapevoli delle potenzialità offerte dagli strumenti informatici e telematici, gli utenti si impegnano ad agire con responsabilità e a non commettere abusi aderendo a un principio di autodisciplina.

La postazione costituita da personal computer viene consegnato completo di quanto necessario per svolgere le proprie funzioni, pertanto è vietato modificarne la configurazione.

Il software installato sui personal computer è quello richiesto dalle specifiche attività lavorative dell'operatore. È pertanto proibito installare qualsiasi programma da parte dell'utente o di altri operatori, escluso l'amministratore del sistema. L'utente ha l'obbligo di accertarsi che gli applicativi utilizzati siano muniti di regolare licenza.

Ogni utente è responsabile dei dati memorizzati nel proprio personal computer. Per questo motivo è tenuto ad effettuare la copia di questi dati secondo le indicazioni emanate dal titolare del trattamento dei dati o suo delegato.

Articolo 3 ABUSI E ATTIVITÀ VIETATE

È vietato ogni tipo di abuso⁵. In particolare è vietato:

- usare la rete in modo difforme da quanto previsto dalle leggi penali, civili e amministrative e da quanto previsto dal presente regolamento;
- utilizzare la rete per scopi incompatibili con l'attività istituzionale del Liceo *Vittorio Emanuele II*;
- utilizzare una password a cui non si è autorizzati;
- cedere a terzi codici personali (USER ID e PASSWORD) di accesso al sistema;
- conseguire l'accesso non autorizzato a risorse di rete interne o esterne a quella del Liceo Vittorio Emanuele;
- violare la riservatezza di altri utenti o di terzi;
- agire deliberatamente con attività che influenzino negativamente la regolare operatività della rete e ne restringano l'utilizzabilità e le prestazioni per altri utenti;
- agire deliberatamente con attività che distruggano risorse (persone, capacità, elaboratori);
- fare o permettere ad altri trasferimenti non autorizzati di informazioni (software, basi dati, ecc.);
- installare o eseguire deliberatamente o diffondere su qualunque computer e sulla rete, programmi destinati a danneggiare o sovraccaricare i sistemi o la rete (p.e. virus, cavalli di troia, worms, spamming della posta elettronica, programmi di file sharing - p2p);
- installare o eseguire deliberatamente programmi software non autorizzati e non compatibili con le attività istituzionali;

⁵ Si intende con abuso qualsiasi violazione del presente regolamento e di altre norme civili, penali e amministrative che disciplinano le attività e i servizi svolti sulla rete e di condotta personale.

- cancellare, disinstallare, copiare, o asportare deliberatamente programmi software per scopi personali;
- installare deliberatamente componenti hardware non compatibili con le attività istituzionali;
- rimuovere, danneggiare deliberatamente o asportare componenti hardware.
- utilizzare le risorse hardware e software e i servizi disponibili per scopi personali;
- utilizzare le caselle di posta elettronica del Liceo Vittorio Emanuele per scopi personali e/o non istituzionali;
- utilizzare la posta elettronica con le credenziali di accesso di altri utenti;
- utilizzare la posta elettronica inviando e ricevendo materiale che violi le leggi.
- utilizzare l'accesso ad Internet per scopi personali;
- accedere direttamente ad Internet con modem collegato al proprio Personal Computer se non espressamente autorizzati e per particolari motivi tecnici;
- connettersi ad altre reti senza autorizzazione;
- monitorare o utilizzare qualunque tipo di sistema informatico o elettronico per controllare le attività degli utenti, leggere copiare o cancellare file e software di altri utenti, senza averne l'autorizzazione esplicita;
- usare l'anonimato o servirsi di risorse che consentano di restare anonimi sulla rete;
- inserire o cambiare la password del bios, se non dopo averla espressamente comunicata all'amministratore di sistema e essere stati espressamente autorizzati;
- abbandonare il posto di lavoro lasciandolo incustodito o accessibile, come specificato nell'allegato 3.

Articolo 4 **ATTIVITÀ CONSENTITE**

È consentito all'amministratore di sistema:

- monitorare o utilizzare qualunque tipo di sistema informatico o elettronico per controllare il corretto utilizzo delle risorse di rete, dei client e degli applicativi, per copiare o rimuovere file e software, solo se rientrante nelle normali attività di manutenzione, gestione della sicurezza e della protezione dei dati e nel pieno rispetto di quanto previsto riguardo ai diritti dei lavoratori;
- creare, modificare, rimuovere o utilizzare qualunque password, solo se rientrante nelle normali attività di manutenzione, gestione della sicurezza e della protezione dei dati e nel pieno rispetto di quanto previsto riguardo ai diritti dei lavoratori. L'amministratore darà comunicazione dell'avvenuta modifica all'utente che provvederà ad informare il custode delle password come da procedura descritta nel DPS;
- rimuovere programmi software, solo se rientrante nelle normali attività di manutenzione, gestione della sicurezza e della protezione dei dati e nel pieno rispetto di quanto previsto riguardo ai diritti dei lavoratori;
- rimuovere componenti hardware, solo se rientrante nelle normali attività di manutenzione, gestione della sicurezza e della protezione dei dati e nel pieno rispetto di quanto previsto riguardo ai diritti dei lavoratori.

Articolo 5 **SOGGETTI CHE POSSONO AVERE ACCESSO ALLA RETE**

Hanno diritto ad accedere alla rete del Liceo *Vittorio Emanuele II*: tutti i dipendenti, le ditte fornitrici di software per motivi di manutenzione e limitatamente alle applicazioni di loro competenza, collaboratori esterni impegnati nelle attività istituzionali per il periodo di collaborazione.

L'accesso alla rete è assicurato compatibilmente con le potenzialità delle attrezzature.

L'amministratore di sistema può regolamentare l'accesso alla rete di determinate categorie di utenti, quando questo è richiesto da ragioni tecniche.

Per consentire l'obiettivo di assicurare la sicurezza e il miglior funzionamento delle risorse disponibili l'amministratore di sistema può proporre al titolare del trattamento l'adozione di appositi regolamenti di carattere operativo che gli utenti si impegnano ad osservare.

L'accesso agli applicativi è consentito agli utenti che, per motivi di servizio, ne devono fare uso.

Articolo 6

MODALITÀ DI ACCESSO ALLA RETE E AGLI APPLICATIVI

Qualsiasi accesso alla rete e agli applicativi viene associato ad una persona fisica cui collegare le attività svolte utilizzando il codice utente.

L'utente che ottiene l'accesso alla rete e agli applicativi si impegna ad osservare il presente regolamento e le altre norme disciplinanti le attività e i servizi che si svolgono via rete ed si impegna a non commettere abusi e a non violare i diritti degli altri utenti e dei terzi.

L'utente che ottiene l'accesso alla rete e agli applicativi si assume la totale responsabilità delle attività svolte tramite la rete.

L'utente è tenuto a verificare l'aggiornamento periodico del software antivirus.

Al primo collegamento alla rete e agli applicativi, l'utente deve modificare la password (parola chiave) comunicatagli dal custode delle password e rispettare le norme indicate nell'allegato 3.

Articolo 7

PROTOCOLLI OPERATIVI

1. Utilizzo del Personal Computer

- a. I Personal Computer affidati al personale di segreteria, ai docenti e agli allievi sono strumenti di lavoro. Ognuno è responsabile dell'utilizzo delle dotazioni informatiche ricevute in assegnazione. Ogni utilizzo non inerente all'attività lavorativa e/o didattica può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza.
- b. Non è consentita l'attivazione della password d'accensione (bios), senza preventiva autorizzazione da parte del D.S. o del D.S.G.A.
- c. Non è consentito all'utente modificare le caratteristiche hardware e software impostate sul proprio PC, salva preventiva autorizzazione del D.S. o del D.S.G.A.
- d. Il Personal Computer deve essere spento prima di lasciare gli uffici o i laboratori o in caso di assenze prolungate dall'ufficio o dal laboratorio.
- e. Le informazioni archiviate informaticamente devono essere esclusivamente quelle previste dalla legge o necessarie all'attività lavorativa e/o didattica.
- f. Negli uffici di segreteria particolare attenzione deve essere prestata alla duplicazione dei dati. È infatti assolutamente da evitare un'archiviazione ridondante.
- g. La tutela della gestione locale di dati sui PC è demandata all'utente finale che dovrà effettuare, con frequenza opportuna, i salvataggi su supporti magnetici e/o di rete e la conservazione degli stessi in luogo idoneo.
- h. Non è consentita l'installazione di programmi diversi da quelli autorizzati dal D.S.
- i. Su richiesta di un docente e per gli usi didattici è possibile installare software aggiuntivo che, in ogni caso, deve essere protetto da licenza d'uso.
- j. Non è consentita la riproduzione o la duplicazione di programmi informatici ai sensi della legge n. 128 del 21.05.2004.

2. Utilizzo della rete LAN

- a. L'accesso alla rete interna è protetto da indirizzi IP dedicati; non è possibile utilizzare propri PC sulla rete d'istituto: chiunque ne voglia far uso deve richiedere i portatili in presidenza o al tecnico di laboratorio informatico;
- b. È fatto divieto di utilizzare la rete interna per fini non espressamente autorizzati;
- c. È vietato connettere in rete stazioni di lavoro se non dietro esplicita e formale autorizzazione del D.S.
- d. È vietato condividere cartelle in rete sia dotate di password, sia sprovviste di password se non dietro esplicita e formale autorizzazione del D.S.
- e. È vietato monitorare ciò che transita in rete.
- f. È vietata l'installazione non autorizzata di modem che sfruttino il sistema di comunicazione telefonico per l'accesso a banche dati esterne o interne all'istituto.

3. Gestione delle password

- a. L'utente è tenuto a conservare con la massima segretezza la parola di accesso alla rete ed ai sistemi e qualsiasi altra informazione legata al processo di autenticazione.
- b. Le persone assegnatarie delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse (art. 615 comma 5 e segg. c.p.).
- c. Nel caso di mittenti sconosciuti o messaggi insoliti, per non correre il rischio di essere infettati da virus, occorrerà cancellare i messaggi senza aprirli.
- d. Nel caso di messaggi provenienti da mittenti conosciuti, ma che contengono allegati sospetti (file con estensione .exe, .scr, .pif, .bat, .cmd), questi ultimi non devono essere aperti.
- e. Evitare che la diffusione incontrollata di "catene di Sant'Antonio" (messaggi a diffusione capillare e moltiplicata) limiti l'efficienza del sistema di posta.
- f. Nel caso in cui si debba inviare un documento all'esterno dell'istituto è preferibile utilizzare un formato protetto da scrittura (ad esempio il formato Acrobat .pdf)
- g. Utilizzare, nel caso di invio di allegati pesanti, i formati compressi (.zip, .rar, .jpg).
- h. L'iscrizione a "mailing list" esterne è concessa solo per motivi professionali, prima di iscriversi occorre verificare in anticipo se il sito è attendibile.
- i. Le caselle di posta devono essere mantenute in ordine, cancellando documenti inutili e soprattutto allegati ingombranti. 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).
- j. L'abilitazione all'aposta esterna ad uso privato deve essere preceduta da regolare richiesta al D.S.
- k. Il contenuto dei messaggi privati di posta elettronica riguarda forme di corrispondenza tutelate dalla Costituzione, dal Codice Penale e dal Codice dell'Amministrazione Digitale.
- l. I docenti sono disciplinarmente responsabili della perdita e/o dello smarrimento della password di accesso al servizio ScuolaNet, per l'inserimento dei dati in piattaforma. Tale password va conservata con estrema cautela.

4. Uso della rete Internet e relativi rischi

- a. L'abilitazione a Internet deve essere preceduta da regolare richiesta al D.S.
- b. Sono a disposizione di personale e non docente (non degli alunni !) due computer nell'antipresidenza: si ricorda a buon fine che è assolutamente proibita la navigazione in Internet per motivi diversi da quelli connessi al servizio scolastico.
- c. Si fa esplicito divieto di servirsi della rete Internet per qualsiasi altra utilizzazione, con particolare riferimento al trattamento di dati personali dell'utente o di terzi.
- d. Non possono essere utilizzati modem privati per il collegamento alla rete.
- e. È vietato l'uso non autorizzato di account, codici di accesso o numeri di identificazione IP.
- f. È fatto divieto all'utente lo scarico di software gratuito (freeware) e shareware prelevato da siti Internet, se non espressamente autorizzato dal D.S.
- g. I minori possono accedere ad Internet solo sotto il controllo diretto di un docente e nei laboratori, non sui computer dell'antipresidenza.
- h. È vietata la partecipazione a Forum non professionali, l'utilizzo di instant messaging e chat, di bacheche elettroniche, di telefonate virtuali e le registrazioni in guest book anche utilizzando pseudonimi o nick name (esclusi gli strumenti autorizzati).
- i. Il Liceo non garantisce la riservatezza dei percorsi compiuti dagli utenti durante la navigazione, che possono essere assoggettati a controllo a fine di rilevazione statistica o ad altri fini previsti per legge.

A norma delle vigenti leggi, l'utente è responsabile civilmente e penalmente per l'uso fatto dell'accesso a Internet. Il Liceo si riserva di denunciare alle autorità competenti l'utente che si renda direttamente responsabile di attività illecite compiute durante la fruizione del servizio.

Il Liceo ha predisposto particolari restrizioni sulla sua rete: ha provveduto al filtraggio del traffico mediante apparati di rete "firewall". Sono filtrati tutti i collegamenti vietati dalla vigente normativa, dalla User Policy del GARR e dalle regole internazionali dell'RFC 1855 "Netiquette Guidelines", nonché quelli verso server, apparati e personal computer non offerenti servizi ufficiali e/o a valenza esterna. Il Liceo garantisce comunque l'accesso a tutte le basi dati presenti in Internet utili alla didattica ad ai servizi amministrativi.

Il presente regolamento può essere suscettibile di modifiche con le stesse modalità previste per la sua approvazione.

Articolo 8
SANZIONI

In caso di abuso, a seconda della gravità del medesimo, e fatte salve ulteriori conseguenze di natura penale, civile e amministrativa, possono essere comminate le sanzioni disciplinari previste dalla normativa vigente in materia e dai regolamenti del Liceo Vittorio Emanuele .

Napoli, 2 dicembre 2011

Il Titolare del trattamento
Prof. Carlo Antonelli

ALLEGATO 2 – Videosorveglianza

Nell'esercitare attività di videosorveglianza, il Liceo Classico Statale “ Vittorio Emanuele II” rispetta il principio di proporzionalità tra i mezzi impiegati ed i fini perseguiti, in particolare si precisa che:

- il trattamento dei dati avviene secondo correttezza e per scopi determinati, espliciti e legittimi;
- l'attività è svolta per la prevenzione di un pericolo concreto o di specifici reati, solo le autorità competenti sono legittimate ad accedere alle informazioni raccolte.

Inoltre l'attività di videosorveglianza è esercitata osservando le seguenti indicazioni:

- sono fornite alle persone che possono essere riprese, indicazioni chiare, anche se sintetiche, circa la presenza di impianti di videosorveglianza;
- è scrupolosamente rispettato il divieto di controllo a distanza dei lavoratori;
- sono raccolti i dati strettamente necessari per il raggiungimento delle finalità perseguite, registrando le sole immagini indispensabili, limitando l'angolo di visuale delle riprese, evitando, quando non indispensabili, immagini dettagliate, ingrandite o con particolari non rilevanti;
- il periodo di conservazione dei dati è limitato allo stretto necessario e non eccede mai i quindici giorni;
- la conservazione dei dati oltre il termine previsto alla lettera d), è possibile solo in relazioni al verificarsi di illeciti o quando siano in corso indagini giudiziarie;
- i dati raccolti per fini determinati non sono utilizzati per finalità diverse o ulteriori, fatte salve le esigenze di polizia o di giustizia e non sono diffusi o comunicati a terzi.

Napoli, 2 dicembre 2011

*Il Titolare del trattamento
Prof. Carlo Antonelli*

