ISTITUTO TECNICO INDUSTRIALE STATALE
"G.GALILEI"

Biotecnologie ambientali . Biotecnologie sanitarie . Chimica e Materiali . Elettronica . Elettrotecnica . Automazione . Informatica e Telecomunicazioni . Meccanica e meccatronica . Energia . Costruzione del mezzo

Via G.Galilei 66 57122 Livorno Tel: 0586 447111 Fax: 0586 447148
e-mail info@galileilivorno.it - www.galileilivorno.it

REGOLAMENTO

PER L'UTILIZZO DI INTERNET,

DELLE APPARECCHIATURE

E DEI LABORATORI INFORMATICI

(Revisione n. 3 – 15 marzo 2017)

SOMMARIO

1. Introduzione

Le attrezzature informatiche e multimediali presenti nella Scuola sono un patrimonio di proprietà esclusiva dell'Istituto Tecnico Industriale «G. Galilei» di Livorno messe a disposizione di tutte le componenti del mondo scolastico, ad ognuna per consentire il perseguimento delle proprie finalità istituzionali, e vanno utilizzate nel rispetto delle norme contenute nel presente Regolamento.
Tali apparecchiature possono essere impiegate esclusivamente per lo svolgimento delle attività didattiche ed amministrative, funzionali alla gestione della scuola. Referenti e responsabili di apparecchiature elettroniche, piattaforme, siti web di proprietà e in dotazione dell'Istituto devono immediatamente segnalare al D.S. eventuali anomalie, perdite di dati, furti, danneggiamenti o manomissioni.
Il curricolo scolastico prevede che gli alunni imparino a trovare materiale, recuperare documenti scambiare informazioni utilizzando le TIC (Tecnologie di Comunicazione Informatica).
I docenti hanno la responsabilità di guidare gli alunni nelle attività on-line, di stabilire obiettivi chiari nell'uso di Internet e insegnarne un uso accettabile e responsabile della rete. L'obiettivo principale resta quello di arricchire ed ampliare le attività didattiche, secondo quanto prevede il curricolo scolastico, l'età e la maturità degli alunni.

Suddette attrezzature, nel seguito anche "Sistemi informatici" o più semplicemente "Sistemi", possono essere classificate, in linea di massima, secondo il seguente elenco esemplificativo e non esaustivo:

- strumenti di formazione a disposizione dei docenti e degli alunni dell'Istituto o degli studenti partecipanti a corsi formativi autorizzati (nel seguito anche più semplicemente "Studenti"), tipicamente installati presso laboratori o aule multimediali (tipicamente aule con videoproiettori, LIM, videoproiettori interattivi o dotate di dispositivi per l'accesso alla rete d'Istituto);
- strumenti di autoformazione e di ricerca a fini didattici ed educativi, in genere presenti in ambienti speciali quali, indicativamente, biblioteca, cineteca, aula di autoformazione, aula di teleconferenza, o dati in dotazione ai singoli docenti, come nel caso dei dispositivi mobili tablet;
- strumenti di lavoro amministrativo, tecnico, direttivo, normalmente presenti presso i vari uffici o in dotazione a laboratori non specificatamente informatici;

- server che forniscono servizi amministrativi, didattici e di controllo degli accessi e del traffico di rete;
- infrastrutture di rete, composte sia da componenti attivi, quali switch, router, access point, che dal cablaggio strutturato e connettività ad Internet.

In tutti i casi l'utilizzazione delle suddette attrezzature:

a. è ammesso esclusivamente per attività di servizio o che abbiano una diretta o indiretta ricaduta sull'efficacia del processo di insegnamento-apprendimento;
b. in nessun caso e modo sarà ammesso un uso privato delle stesse;
c. comporta l'accettazione incondizionata del presente Regolamento.

Sarà cura e responsabilità della Dirigenza Scolastica rendere noto a tutte le componenti della scuola questo Regolamento attraverso la più ampia diffusione e verificarne la puntuale applicazione da parte di tutti gli operatori dell'Istituto Tecnico Industriale «G. Galilei» di Livorno.

2. Campo di applicazione e riferimenti

L'attività operativa svolta mediante l'uso di attrezzature informatiche e multimediali coinvolge, direttamente o indirettamente, aspetti che riguardano

- la Sicurezza sul posto di lavoro;
- la tutela della Privacy nella gestione dei dati mediante sistemi informatici;
- il Controllo del Traffico di rete;
- la Gestione dei Sistemi Informatici e delle Reti Dati (hardware, software, sicurezza dei dati e dei sistemi);
- le norme di Accesso e di Uso;
- le norme di Comportamento.

Il presente Regolamento esplicita le norme che regolano:

a. l'accesso agli ambienti contenenti attrezzature informatiche e multimediali e ai servizi di rete;
b. l'uso delle attrezzature informatiche e delle reti;
c. le norme comportamentali da tenersi sia quando si accede ai vari ambienti, sia quando si utilizzano i servizi di rete, questi ultimi soprattutto in relazione ad una corretta gestione della privacy e della sicurezza dei dati.

Per gli altri aspetti elencati in precedenza si rimanda alla normativa di riferimento e ai relativi documenti redatti dall'I.T.I.S. G. Galilei che integrano e completano quanto non esplicitamente indicato nel presente Regolamento.

3. Definizioni, sigle e abbreviazioni

Nella presente regolamento si utilizzano le seguenti abbreviazioni:

SIGLA	SIGNIFICATO
ADM	Amministratore di un sistema informatico (server o stazione di lavoro - PC)
ALU	Alunno istituzionale
ATA	Amministrativo Tecnico Ausiliario
COORD	Coordinatore gruppo Disciplinare o Dipartimentale o di Indirizzo / Articolazione
CVP	Collaboratori del DS in Vicepresidenza
DOC	Docente (Insegnante Teorico o Insegnante Tecnico Pratico)
DS	Dirigente scolastico
DSGA	Direttore dei Servizi Generali ed Amministrativi
ITP	Insegnante Tecnico Pratico
INS	Insegnante Teorico
RefAULA	Referente Aula aumentata dalla tecnologia (Aula Multimediale)
RefSERVER	Referente per il Server
RefLAB	Referente di Laboratorio
RefWEB	Referente per il WEB: sito ufficiale di Istituto, caselle postali istituzionali, Albo on-line e Amministrazione Trasparente
RGSI	Referente Gestione dei Sistemi Informatici
RLS	Rappresentante dei lavoratori per la sicurezza
RSPP	Responsabile del Servizio di Prevenzione e Protezione
STUD	Studente Partecipante a corso di formazione o di aggiornamento
TecLAB	Tecnico di Laboratorio
TecSU	Tecnico con compiti di manutenzione e supporto per i Servizi e gli Uffici
TecWEB	Tecnico per il WEB
UTA	Ufficio Tecnico Amministrativo
RUTA	Responsabile UTA

4. Gestione tecnica delle attrezzature informatiche

La gestione della attrezzature informatiche e dei servizi di rete dell'ITIS G. Galilei è di competenza del DS che, a livello tecnico, si avvale della collaborazione di un Team Tecnico di personale specializzato interno all'Istituto cui conferisce, all'inizio di ogni Anno Scolastico e per iscritto, gli opportuni incarichi. L'incarico deve essere controfirmato "per accettazione" dalla persona individuata.

Il Team Tecnico è di norma composto:

a. dal Referente Gestione dei Sistemi Informatici (RGSI), con funzione di coordinamento;

b. dai Tecnici di Laboratorio (TecLAB);
c. dai Tecnici con compiti di manutenzione e supporto per i Servizi e gli Uffici (TecSU);
d. dai Referenti della Aule aumentate dalla tecnologia (Aule Multimediali) (RefAULA);
e. dai Referenti dei Server (RefSERVER);
f. dai Referenti dei laboratori con attrezzature informatiche (RefLAB);
g. dal Referente per il WEB (RefWEB).

Ogni componente del Team Tecnico (indicato nel seguito anche “Amministratore di sistema” o più semplicemente “Amministratore”), ognuno per la parte di propria competenza, provvedere all'installazione, configurazione, manutenzione e amministrazione tecnica dei sistemi informatici e delle componenti di rete ad esso assegnati in conformità a quanto specificato nel "Documento Programmatico della Sicurezza" e nel documento di "Gestione dei Sistemi Informatici e delle Reti" e alle disposizioni di legge relative al Codice in materia di protezione dei dati personali (D.Lgs. 196/2003, così detta Legge sulla Tutela della Privacy) e alla legge sulla Sicurezza nei luoghi di lavoro (D.lgs 81/08).
Di seguito si riassumono alcuni dei principali compiti assegnati ad un Amministratore di sistema.
Solo se rientranti nelle normali attività di manutenzione e gestione dei sistemi, della sicurezza e della protezione dei dati, all'amministratore di sistema è consentito:

1. 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;
2. creare, modificare, rimuovere o utilizzare qualunque password; generare i codici di autorizzazione (password temporanee) per i nuovi utenti nel rispetto delle regole di composizione descritte nel già richiamato documento di "Gestione dei Sistemi Informatici e delle Reti"; cancellare e/o annullare le password scadute, gli utente e le password degli utenti che non hanno più i requisiti necessari per accedere al sistema;
3. rimuovere o installare software e componenti hardware;
4. accedere a quella parte del sistema informativo necessaria per espletare la funzione amministrativa, limitando l'accesso in via esclusiva all’ambito, alla categoria di dati, alle modalità e al tempo strettamente necessario per espletare l'intervento manutentivo e in accordo alla nomina di “incaricato al trattamento dati” che necessariamente un amministratore di sistema dovrà avere da parte del responsabile del trattamento dati dell'Istituto;

5. pianificare e configurare le operazioni di backup del server amministrativo, controllare il suo corretto funzionamento e verificare periodicamente la consistenza e la congruità dei contenuti delle copie di backup;
6. gestire i sistemi di autenticazione e di autorizzazione per l'accesso alla rete dell'Istituto, cablata e wireless, e configurare i criteri di autenticazione;
7. stabilire la condivisione o meno in rete di risorse, hardware e software, in base a quanto stabilito nel Documento Programmatico sulla Sicurezza;
8. progettare l'architettura di rete e monitorare la struttura e gli apparati di rete;
9. in coerenza con l'ambiente nel quale un sistema informatico deve operare e con le funzionalità che esso deve fornire all'utente, definire e realizzare un'adeguata configurazione hardware e software;
10. intervenire in caso di problemi o guasti, eventualmente contattando il manutentore hardware/software e seguendo le operazioni che esso effettua;
11. pianificare migliorie al Sistema Informatico;
12. controllare il corretto funzionamento della rete e delle risorse hardware e software condivise ed eventualmente pianificare interventi da parte di tecnici specializzati esterni e, in caso di loro intervento, seguire le operazioni che vengono compiute;
13. impartire istruzioni per la corretta applicazione delle norme vigenti in materia di sicurezza informatica agli utenti del sistema informativo e, se autorizzato dal titolare e/o responsabile del trattamento dei dati, impartire disposizioni operative per la sicurezza delle banche dati e dei procedimenti di gestione e/o trattamento degli stessi.
14. assicurarsi che su tutti i sistemi informatici ci sia installato e costantemente aggiornato software antivirus e antimalware, definire ed impostare la loro configurazione e le regole di sicurezza per i browser utilizzati per navigare su Internet;
15. impostare le regole di filtraggio del traffico di rete e per l'accesso ad Internet;
16. segnalare al responsabile del trattamento dati le eventuali violazioni della policy di uso delle credenziali di autenticazione;
17. segnalare al DS eventuali violazioni della policy di navigazione di rete.

5. Norme per l'accesso agli ambienti e ai servizi

5.1 AMBIENTI CON ATTREZZATURE INFORMATICHE E MULTIMEDIALI

Gli ambienti con attrezzature informatiche e multimediali presenti in Istituto sono classificati nelle seguenti tipologie:

a. Laboratori;
b. Aule aumentate dalle tecnologie (Aule aumentate o Aule multimediali);
c. Aule speciali;
d. Centro di Calcolo;

L'accesso a tutti gli ambienti che presentano attrezzature informatiche e multimediali è implicitamente e generalmente consentito alle seguenti figure:

1. Dirigente Scolastico (DS);
2. Direttore dei Servizi Generali e Amministrativi (DSGA);
3. Collaboratori del DS in Vicepresidenza (CVP);
4. Referente Gestione dei Sistemi Informatici (RSGI);
5. Responsabile dell'Ufficio Tecnico Amministrativo (RUTA);
6. Responsabile del Servizio di Prevenzione e Protezione (RSPP);
7. Rappresentanti dei Lavoratori per la Sicurezza (RLS);
8. Coordinatore di Indirizzo/Articolazione/Gruppo disciplinare cui fa eventualmente capo l'ambiente (COORD).
9. Personale Tecnico in organico nell'ambiente di riferimento (TecLAB) o incaricato della gestione tecnica della strumentazione informatica presente nell'ambiente (TecSU);
10. Collaboratori scolastici in organico nell'ambiente di riferimento;
11. Collaboratori scolastici latori di comunicazioni (es. circolari).

A queste figure se ne aggiungono altre ugualmente autorizzate implicitamente e che vengono dettagliate nel seguito del presente regolamento per ogni tipologia di ambiente.

Limitatamente agli ambienti appartenenti alle tipologie Laboratori, Aule Multimediali e Aule Speciali, è consentito l'accesso da parte di persone diverse da quelle implicitamente autorizzate, solo se espressamente autorizzate dal DS, o da suo delegato (o dal RefLAB o dal COORD nel caso di Laboratorio), purché per:

- scopi didattici e/o formativi;
- manutenzione specialistica;

- sperimentazioni di soluzioni hardware e software preventivamente concordate con il RefLAB e il COORD (solo per gli ambienti che fanno capo a tali figure);
- per l'esecuzione di gare o di concorsi da svolgersi con l'ausilio di strumentazione informatica.

Suddette autorizzazioni sono gestite dal DS, o suo delegato, e, in ogni caso, non possono pregiudicare lo svolgimento delle attività didattiche istituzionali assegnate all'ambiente che, pertanto, hanno di norma la precedenza su tutte le altre attività.

E' consentito accedere agli ambienti che presentano attrezzature informatiche anche in occasione di riunioni di organi collegiali scolastici, ad esempio Consigli di Istituto, Consigli di Classe, Riunioni di Gruppi Disciplinari e Dipartimentali, riunioni di Commissioni istituite dal Collegio dei docenti o dal DS. In questi ultimi casi l'autorizzazione all'accesso avviene di norma sulla base di esplicita circolare emanata dalla Presidenza e si estende a tutti i componenti dell'organo collegiale.

Le chiavi per l'accesso ai vari ambienti sono in dotazione al personale ausiliario incaricato, che provvede all'apertura del locale solo in presenza di attività programmata e autorizzata e, nel caso di laboratorio, in presenza del docente con la classe o per quei docenti che ne fanno richiesta e che normalmente operano nel laboratorio. Al termine dell'attività il personale ausiliario effettuerà una ricognizione visiva dell'ambiente per verificare che tutto risulti in ordine. In ogni caso i locali non dovranno rimanere aperti in assenza di attività istituzionale, pianificata e autorizzata.

5.1.1 LABORATORI

In aggiunta alle figure elencate all'inizio del par. 5.1, l'accesso ai laboratori è implicitamente consentito anche a:

1. Referente del Laboratorio (RefLAB);
2. Docenti (DOC) che svolgono attività didattica nel laboratorio;
3. Alunni (ALU), limitatamente agli orari di svolgimento delle esercitazioni didattiche;
4. Partecipanti a corsi formativi (STUD), limitatamente agli orari di svolgimento dei corsi di formazione o di aggiornamento.

All'inizio dell'Anno Scolastico, successivamente alla pubblicazione dell'orario ufficiale definitivo, ogni Dipartimento, sentito il parere dei TecLAB, può strutturare un "Piano di Utilizzazione" dei laboratori che fanno capo al Dipartimento, da parte dei docenti che insegnano discipline di indirizzo, in ore durante le quali i laboratori non sono allocati nell'orario

ufficiale definitivo e non sono oggetto di manutenzione ordinaria. Tale piano deve essere sottoposto all'approvazione del DS.

I docenti che svolgono normalmente attività didattica nel laboratorio possono pianificare, coordinandosi con gli altri docenti che insistono sul laboratorio, sentito il parere del TecLAB e acquisito il parere favorevole del RefLAB o del Coordinatore del Dipartimento cui il laboratorio fa capo, rientri pomeridiani con alunni dell'indirizzo per lo svolgimento di attività didattiche connesse a progetti approvati nell'ambito dipartimentale o dai Consigli di Classe delle classi appartenenti al Dipartimento.

In tutti i casi, l'accesso di alunni e studenti al laboratorio è consentito solo alla presenza di un docente accompagnatore che applica il regolamento e che si assume la responsabilità di gestire la struttura tecnologica e di vigilare sul suo corretto utilizzo.

5.1.2 AULE AUMENTATE DALLE TECNOLOGIE (ANCHE AULE AUMENTATA)

L'accesso alle aule aumentate è implicitamente consentito anche a:

1. Referenti della Aula aumentata (RefAULA);
2. Docenti (DOC) che svolgono attività didattica nell'aula;
3. Alunni (ALU), limitatamente agli orari di svolgimento delle attività didattiche;
4. Partecipanti a corsi formativi (STUD), limitatamente agli orari di svolgimento dei corsi di formazione o di aggiornamento.

Ogni docente può richiedere al DS, o suo delegato, l'autorizzazione ad utilizzare un'aula aumentata per svolgere attività didattica con una classe, o gruppi di alunni, per un determinato periodo di tempo e relativamente ad ore durante le quali l'ambiente non è allocato nell'orario ufficiale definitivo e non è impegnato altrimenti, presentando un "Piano di Utilizzazione personale".

Con le stesse modalità precedentemente esposte, ogni docente può pianificare rientri pomeridiani in un'aula aumentata con alunni dell'Istituto o studenti che partecipano a corsi di formazione e per sole finalità didattiche connesse a progetti approvati dall'Istituto o a livello dipartimentale o di Consiglio di Classe.

Anche in questi casi, l'accesso degli alunni e studenti all'aula aumentata è consentito solo alla presenza del docente accompagnatore che applica il regolamento e che si assume la responsabilità di gestire la struttura tecnologica e di vigilare sul suo corretto utilizzo.

5.1.3 AULE SPECIALI

Appartengono a questa categoria di ambienti la Biblioteca, la Cineteca, l'aula di Autoformazione dei docenti, l'aula di Teleconferenza.

L'accesso a queste aule speciali è implicitamente consentito anche a:

1. docenti che svolgono attività di autoformazione, studio e ricerca che abbiano una diretta o indiretta ricaduta sull'efficacia dei processo di insegnamento-apprendimento (Biblioteca, Teleformazione);
2. docenti, alunni, studenti, ATA per attività connesse direttamente o indirettamente al processo di insegnamento-apprendimento (Biblioteca, Cineteca, Teleconferenza).

L'accesso a Biblioteca, Cineteca e Teleconferenza è autorizzato dal DS, o da suo delegato, che all'inizio di ogni Anno Scolastico definisce e regolamenta un adeguato ed efficace meccanismo di prenotazione, affidandone la gestione a personale interno all'Istituto.

L'accesso di alunni e studenti a Cineteca e Teleconferenza può avvenire solo in presenza del docente che ha prenotato l'ambiente.

5.1.4 UFFICI

L'accesso agli uffici è implicitamente consentito anche a:

1. tutto il personale amministrativo.

E' consentito l'accesso da parte di persone diverse da quelle implicitamente autorizzate solo se espressamente autorizzate dal DS, o da suo delegato, e per eseguire installazioni hardware e software o per manutenzione specialistica.

5.1.5 CENTRO DI CALCOLO

L'accesso al Centro di Calcolo è implicitamente consentito anche a:

1. amministratori dei server presenti in esso.

E' consentito l'accesso da parte di persone diverse da quelle implicitamente autorizzate solo se espressamente autorizzate dal DS, o da suo delegato, e per eseguire installazioni hardware e software o per manutenzione specialistica. Vista la centralità del Centro di Calcolo nel funzionamento di tutti i servizi dati e della rete di Istituto, l'accesso delle persone autorizzate precedentemente richiamate può avvenire solo in presenza del RGSI o di suo delegato.

5.2 SERVIZI DATI E DI RETE

E' consentito usufruire dei servizi di rete unicamente per scopi didattici o che abbiamo una ricaduta diretta o indiretta sull'efficacia del processo di insegnamento-apprendimento, comprese le attività istituzionali amministrative e di gestione del sistema di relazioni dell'ITIS G. Galilei. Tutto il personale della scuola, gli alunni e gli studenti hanno la possibilità di accedere alla rete dati cablata di Istituto, e quindi a tutte le risorse messe esplicitamente a loro disposizione, ivi compresa la navigazione su Internet, ma nel rispetto delle norme di legge e

secondo modalità e autorizzazioni che differiscono a seconda della categoria di utenza cui essi appartengono e coerentemente alla politica di sicurezza definita dalla Dirigenza Scolastica e implementata dal Team Tecnico, ognuno per la sua parte, con la collaborazione dei Coordinatori di Indirizzo/Articolazione/Gruppo disciplinare.

La rete WiFi di istituto al momento è accessibile sono al personale e in particolar modo ai docenti che hanno l'esigenza di connettività mobile derivante dall'adozione del Registro Elettronico, salvo rare eccezioni autorizzate dal DS, o suo delegato.

In relazione alle modalità di accesso, al momento al momento sono previste le seguenti tipologie:

1. l'accesso alla rete cablata degli uffici e ai suoi servizi è regolato da autenticazione basata su coppia ("NOME UTENTE", "PASSWORD); il “NOME UTENTE” viene dato in uso all’utente che non può in alcun modo considerarlo come proprietà privata ed è l'unica informazione che può liberamente essere resa pubblica mentre la “PASSWORD”, inizialmente impostata dall'amministratore del sistema di gestione degli accessi, deve essere personalizzata dall'utente con una di propria scelta e deve essere immessa direttamente dallo stesso in modo non trasparente ad altri;
2. l’accesso alla rete cablata dei laboratori e delle aule speciali da parte di studenti e docenti, non presentando problematiche di sicurezza e privatezza di dati sensibili o importanti, avviene tramite inserimento di coppia ("NOME UTENTE", "PASSWORD) che, però, è unica per ogni ambiente ed è condivisa. Il flusso dei dati viene, tuttavia, controllato con opportuni filtri sui siti e i contenuti;
3. l’accesso alla rete WiFi di Istituto è basato, a seconda dei casi e delle finalità didattiche da prseguire, su coppia ("NOME UTENTE", "PASSWORD) validate da un sistema di autentificazione Radius e crittografia WPA2-Enterprise o su chiave condivisa e crittografia WPA2.

E' vietato ad ogni utente fornire ad altri indicazioni o istruzioni che possano essere idonee a consentire l’accesso al sistema informatico, ai servizi dati e di rete dell'ITIS G. Galilei.

Il DS, secondo tempistiche casuali e nel rispetto della normativa cogente, può procedere a verifiche a campione e, in caso di attività sospetta, prendere visione e conoscenza dei dati legati ai singoli utenti (contenuto dei sistemi utilizzati, delle cartelle su di essi e di quella personale, tracce di tutte le attività svolte, siti visitati ecc.) e dare mandato al RGSI di revocare l’uso delle attrezzature.

Il personale che ottiene la coppia di accesso deve essere a conoscenza di quanto incluso in tale regolamento ed accettarne le condizioni in modo incondizionato, fatte salve le norme relative alla Legge di Tutela della Privacy. In caso di violazioni reiterate, o di particolare gravità, o dolo manifesto, il DS potrà provvedere con azioni disciplinari ed eventuali azioni legali, oltre ad intraprendere tutte le azioni necessarie ad ottenere il rimborso delle spese per gli eventuali danni causati, di qualsiasi natura essi siano.

Nella tabella che segue sono riassunte le autorizzazioni di accesso ed uso dei servizi dati e di rete per le varie categorie di utenza presenti dell'ITIS G. Galilei.

Utenti	Accesso rete cablata	Accesso rete WiFi	Accesso Server Amministrativo	Accesso Server Didattici	Accesso PC Laboratorio	Navigazione Internet
Area Dirigenza	SI	SI	SI	SI	SI	SI (continua)
Personale Amm.vo	SI	A richiesta (su autorizz. DS)	SI	NO	NO	SI (continua)
Personale Tecnico	SI	A richiesta (su autorizz. DS)	NO	NO	SI	SI (continua)
Personale Ausiliario	SI	A richiesta (su autorizz. DS)	NO	NO	NO	SI (continua)
Docenti	SI	SI	NO	SI	SI	SI (continua)
Alunni e Studenti Partecipanti	SI	NO (SI su autorizz. DS)	NO	NO	SI (su autor. DOC)	SI (regolamentata da DOC)
Famiglie e visitatori	NO (SI su autorizz. DS e da postazioni stabilite)	NO	NO	NO	NO	NO (SI su autorizz. DS e da postazioni stabilite)

6. Norme per l'utilizzazione delle attrezzature informatiche e per l'accesso agli ambienti con attrezzature informatiche

Un uso non corretto delle attrezzature informatiche o assumere comportamenti non adeguati o corretti negli ambienti che presentano tali attrezzature può non solo determinare un pericolo immediato per la salute propria o di altri, ma anche pregiudicare il corretto funzionamento delle

attrezzature stesse, fino alla loro rottura, o anche determinare l'insorgenza di serie problematiche di sicurezza e privatezza dei dati con risvolti che, a seconda dei casi, possono condurre fino a rilievi di tipo civile e penale.

Per questi motivi chiunque utilizza attrezzature informatiche e/o accede ad ambienti dotati di tali tipi di attrezzature e/o accede alla rete d'Istituto, sia essa la rete cablata che la rete WiFi, deve uniformarsi alle regole specificate nel presente regolamento consapevole che il loro mancato rispetto può comportare, a giudizio del DS, la sospensione temporanea o definitiva dell'accesso agli ambiente, all'uso delle attrezzature informatiche e dei servizi dati e di rete.

In aggiunta, visto che di qualsiasi operazione effettuata su di un computer resta traccia scritta sul disco rigido, analizzabile da personale tecnico competente con le moderne tecniche di indagine informatiche, a discrezione del DS ogni abuso, o presunto tale, potrà essere verificato e controllato, nel rispetto della legge sulla tutela della privacy, e potranno essere assunti i provvedimenti più idonei nei confronti di coloro che se ne saranno resi responsabili

6.1 REGOLE DI ACCESSO E DI USO

In relazione all'uso delle attrezzature, ivi compreso l'accesso e l'utilizzazione della rete dati (cablata e WiFi), valgono le seguenti regole:

1. è proibito agli alunni e ai studenti accedere ai laboratori con attrezzature informatiche, nelle aule speciali e negli uffici in assenza del docente o del personale preposto;
2. è vietato a chiunque utilizzare software in violazione alla legge sul COPYRIGHT, e quindi di installare e/o usare software non conforme a tale legge o comunque non regolarmente licenziato c/o l'Istituto; ogni conseguenza derivante dalla violazione a tale divieto ricadrà unicamente su chi ha compiuto l'illecito e su eventuali fruitori di tali software; chiunque venisse a conoscenza della presenza su una qualsiasi macchina di software detenuto illegalmente ha l'obbligo di informare immediatamente il Referente dell'ambiente nel quale è presente tale software o, in mancanza di questo, il personale preposto alla gestione e manutenzione tecnica dell'ambiente, il RGSI, il DS, o persona da esso delegata;
3. fatti salvi quanto specificato al paragrafo 4 sui compiti e le prerogative del Team Tecnico e i casi i cui siano pianificate attività didattiche specialistiche (soprattutto nell'indirizzo Informatica) svolte sotto il diretto controllo del docente, è fatto divieto assoluto e totale a chiunque di installare e/o usare software atti a consentire l'accesso non autorizzato ai sistemi (per es. "backdoor", "cavalli di troia", ecc.), a recuperare password, a intercettare

e/o controllare il traffico di rete, ad analizzare i flussi per scoprire password e/o dati personali, a condurre attacchi informatici di qualsiasi natura ed entità a sistemi sia interni all'Istituto che di terze parti; ogni conseguenza derivante dalla violazione a tale divieto ricadrà unicamente su chi ha compiuto l'illecito e su eventuali fruitori di tali software; chiunque venisse a conoscenza della presenza su una qualsiasi macchina di tali software ha l'obbligo di informare immediatamente il Referente dell'ambiente nel quale è presente tale software o, in mancanza di questo, il personale preposto alla gestione e manutenzione tecnica dell'ambiente, il RGSI, il DS, o persona da esso delegata;

4. è vietato l'uso e l'installazione di programmi software senza l'autorizzazione esplicita del responsabile dell'ambiente;
5. è vietata qualsiasi attività di download di software, dati, contenuti di qualsiasi natura che non abbiamo un legame diretto o indiretto con il processo di insegnamento-apprendimento, nel caso di laboratori o aule, e con la corretta funzionalità del software gestionale, nel caso degli uffici;
6. è vietato l'utilizzo delle stampanti per uso privato e utilizzarle per produrre più copie dello stesso materiale didattico da distribuire ad alunni o studenti, in questi casi è necessario usufruire del servizio di fotocopiatrice messo a disposizione dall'Istituto;
7. è vietato agli alunni e agli studenti l'uso delle stampanti senza l'autorizzazione esplicita del docente;
8. è vietato intervenire personalmente in caso di guasto o ordinaria manutenzione delle risorse; in questi casi occorre rivolgersi al personale tecnico preposto;
9. è vietato alterare le apparecchiature e spostarle dalla loro posizione originale senza esplicita autorizzazione del DS, o suo delegato, o dal RefLAB o dal COORD nel caso di Laboratorio;
10. e vietato effettuare cablaggi su tutte le apparecchiature e periferiche;
11. è vietato l'utilizzo di attrezzature personali (es. portatili, tablet, dispositivi USB esterni, ecc.) senza l'autorizzazione del responsabile dell'ambiente;
12. nel caso di personale amministrativo, l'accesso ai dati sulla rete d'Istituto deve essere conforme alla delega ottenuta da ognuno di essi nell'ambito del sistema di gestione della privacy attuato dall'ITIS G. Galilei;
13. nel caso di personale docente, l'accesso ai dati sulla rete d'istituto deve essere limitata ai soli dati relativi ai propri alunni o studenti e in conformità alle finalità proprie della

funzione docente e del ruolo che egli ricopre in seno al Consiglio di Classe (es. Coordinatore);

14. nel caso di alunni o studenti, l'accesso ai dati sulla rete d'Istituto è limitato a soli componenti software messi a loro disposizione dal docente o relativi ad esperienze riconducibili al processo di apprendimento (es. dati di esercitazioni, informazioni su eventi, sequenze audio-video con valenza didattica ed autorizzati dal proprio docente, ecc.);
15. nel caso in cui, per qualsiasi motivo, tecnico, malfunzionamento delle attrezzature, ecc., si avesse accesso a dati per i quali non si ha esplicito o implicito permesso di accesso, è assolutamente obbligatorio desistere immediatamente dal proseguire nella loro visione ed informare dell'accaduto il responsabile dell'ambiente in cui è avvenuto l'evento;
16. gli accessi alle risorse su Internet devono essere effettuate nel rispetto delle disposizioni di legge, di regolamento interno e delle regole di filtraggio del traffico stabilite nell'ambito della politica di sicurezza dell'ITI G. Galilei ed è fatto divieto assoluto intraprendere qualsiasi attività o mettere in atto comportamenti atti a by-passare il controllo del flusso nella navigazione;
17. nel caso di personale docente o ATA, la navigazione su Internet avviene sotto la loro diretta responsabilità, fatta salva la prerogativa del DS di eseguire controlli casuali a campione sulle attività svolte secondo quanto già specificato nel paragrafo 4.2 per l'accesso ai servizi dati e di rete;
18. nel caso di alunni o studenti, la navigazione su Internet avviene sotto stretto controllo del personale di laboratorio e del docente; in qualunque momento il docente o il responsabile dell'ambiente che verifichino un uso della connessione contrario a disposizioni di legge o di regolamento interno, e comunque non coerente con i principi che regolano il controllo del flusso di navigazione stabilite nell'ambito della politica di sicurezza dell'ITI G. Galilei, devono disattivarla senza indugio e darne comunicazione al Coordinatore del Consiglio di Classe di loro appartenenza per l'adozione di eventuali provvedimenti disciplinari;
19. in base alle leggi che regolano la distribuzione delle licenze, i prodotti software presenti in laboratorio non sono disponibili per il prestito individuale;
20. è vietato copiare i programmi installati sulle macchine su qualunque tipo di supporto, né per uso personale, né per uso professionale né per uso commerciale, né in tutto né in parte, né per un utilizzo permanente né per un utilizzo temporaneo;

21. è vietato modificare, tradurre, adattare, trasformare i programmi installati sulle macchine;
22. ogni utente si obbliga a non diffondere programmi virus o comunque idonei ad arrecare danno ai sistemi informatici dell'Istituto o a sistemi informatici altrui;
23. ogni utente si obbliga a non lasciare supporti di memorizzazione esterni (es. penne USB), cartelle o altri documenti a disposizione di estranei
24. gli eventuali utilizzatori esterni occasionali, debitamente autorizzati all'accesso secondo quanto specificato nel relativo paragrafo del presente regolamento, devono:
    - rapportarsi col responsabile dell'ambiente (RefLAB, RefSU, COORD, RGSI), prima di utilizzare le apparecchiature, al fine di organizzare al meglio le attività da svolgere senza pregiudicare in alcun modo il normale utilizzo dell'ambiente e delle sue attrezzature;
    - rispettare scrupolosamente il presente regolamento.

6.2 REGOLE COMPORTAMENTALI

Coloro che assumono un comportamento inadeguato in un ambiente con attrezzature di qualsiasi genere, comprese anche quelle di natura informatica, non mettono a repentaglio solo la propria salute, ma anche quella degli altri.

Pertanto in questi ambienti è obbligatorio assumere un comportamento che si uniformi alle direttive esplicitate nel seguito:

1. quando si accede per la prima volta ad un ambiente con attrezzature informatiche e non si è quindi avvezzi all'uso della stesse è obbligatorio contattare prima il responsabile dell'ambiente e il personale tecnico cui è affidata la manutenzione per informarsi sulla situazione delle attrezzature, la disponibilità del software, le regole di utilizzo;
2. leggere e rispettare sempre le indicazioni dei cartelli di segnalazione e informazione posti sulle attrezzature e strumentazioni presenti nei vari ambienti;
3. è fatto divieto assoluto intraprendere qualsiasi attività che conduca all'accesso, all'utilizzazione e alla conoscenza di dati che non rientrano tra quelli per i quali si abbia esplicito o implicito permesso di accesso;
4. non sono ammesse attività di tipo ricreativo e pertanto è vietato accedere a siti web o fare uso di software non strettamente connessi alle finalità istituzionali dell'Istituto (come, per esempio non esaustivo, giochi software, programmi di chat, messaggistica istantanea per scopi personali, ecc.);

5. usare con cura le attrezzature e le apparecchiature seguendo le indicazioni dei docenti e del personale tecnico preposto, nel caso di alunni e studenti, degli amministratori di sistema e del personale tecnico preposto, nel caso di personale docente o ATA;
6. segnalare al personale preposto alla gestione e manutenzione tecnica dell'ambiente eventuali danni e/o malfunzionamenti delle apparecchiature;
7. tenere comportamenti tali da ridurre il rischio di attacco al sistema informatico mediante virus o ogni altro software aggressivo (ad esempio non aprire mail o relativi allegati sospetti, non navigare su siti non professionali ecc..);
8. controllare la presenza e il regolare funzionamento del software antivirus e nel caso in cui il software antivirus rilevi la presenza di un virus che non è riuscito ad eliminare, sospendere immediatamente ogni elaborazione in corso senza spegnere il computer e segnalare l'accaduto al responsabile dell'ambiente;
9. controllare mediante il programma antivirus installato sui vari sistemi ogni dispositivo magnetico di provenienza esterna all'Istituto prima del suo utilizzo e, nel caso venga rilevato un virus non eliminabile dal software, desistere dall'utilizzarlo;
10. non cercare di fare funzionare apparecchiature che non si conoscono;
11. non toccare con le mani bagnate apparecchi elettrici sotto tensione;
12. sono assolutamente proibiti scherzi di qualsiasi genere e atteggiamenti lesivi della personalità propria o altrui;
13. nei vari ambienti è assolutamente vietato bere, mangiare, correre, aprire o chiudere violentemente le porte, sedersi o sdraiarsi sui banchi di lavoro, ecc.;
14. i passaggi tra gli arredi (banchi, scrivanie, ecc.) e verso le porte, le porte stesse, i corridoi e tutte le vie di fuga devono essere sempre tenuti sgombri, i cassetti degli arredi e gli armadietti devono essere tenuti chiusi (borse, libri abiti ombrelli ecc. devono essere lasciati negli appositi spazi);
15. alla fine di ogni attività svolta con l'ausilio di strumentazione informatica, attenersi scrupolosamente alle procedure di spegnimento dettate dal responsabile dell'ambiente o dal personale tecnico responsabile della loro manutenzione;
16. di norma non è consentito lasciare il posto VDT senza aver preventivamente attivato la procedura di disattivazione;
17. nel caso di esercitazioni svolte da alunni o studenti che partecipano a corsi di formazione, i docenti, al termine dell'attività, dovranno:

- effettuare una ricognizione dell'ambiente e delle attrezzature segnalando immediatamente ogni eventuale guasto, manomissione, danneggiamento, furto ecc., al responsabile dell'ambiente;
- verificare il corretto spegnimento delle attrezzature;

18. in occasione di particolari situazioni come manifestazioni, occupazione studentesca, autogestione, l'accesso ad ambienti datati di strumentazioni informatiche è assolutamente interdetto ai manifestanti, salvo specifiche indicazioni del DS, o suo delegato.
19. in relazione alle password, ogni utente si obbliga a scegliere una password con le seguenti caratteristiche minime:
    - originale;
    - composta da otto caratteri;
    - che contenga almeno tre dei seguenti quattro gruppi: caratteri maiuscoli; caratteri minuscoli, cifre, segni di interpunzione e/o caratteri speciali;
    - che non sia facilmente intuibile, evitando il nome proprio, il nome di congiunti, date di nascita e comunque riferimenti alla propria persona o lavoro facilmente ricostruibili
20. in relazione alla posta elettronica, ogni utente si impegna ad utilizzare le seguenti regole minime:
    - non aprire documenti di cui non sia certa la provenienza;
    - non aprire direttamente gli allegati ma salvarli su disco e controllarne il contenuto con un programma antivirus;
    - controllare accuratamente l'indirizzo dei destinatario prima di inviare dati personali;

7. Uso di internet da parte del personale dipendente

Tutti i dipendenti possono utilizzare Internet.

Il dipendente-utente è direttamente e totalmente responsabile dell'uso che egli fa del servizio di accesso ad Internet, dei contenuti che vi ricerca, dei siti che contatta, delle informazioni che vi immette e delle modalità con cui opera.

L'uso di Internet nelle numerose funzionalità è consentito esclusivamente per scopi attinenti alle proprie mansioni.

Al dipendente non è consentito:

1. caricare/scaricare (upload/download) da Internet files musicali, video o software che non siano attinenti alla propria mansione, come anche l'utilizzo di connessione ad Internet per motivi strettamente personali, in quanto ciò si configura come danno patrimoniale cagionato all'Amministrazione consistente nel mancato svolgimento della prestazione lavorativa durante il periodo di connessione;
2. l'utilizzo delle risorse del server centrale per la memorizzazione di materiale di uso privato, personale o non attinente alla attività lavorativa;
3. effettuare transazioni finanziarie, operazioni di remote banking, acquisti on-line e simili, se non attinenti l'attività lavorativa o direttamente autorizzati dal Responsabile;
4. utilizzare sistemi Peer to Peer, di file sharing, podcasting, web casting, eMule, utorrent e similari, così come connettersi a siti che trasmettono programmi in streaming (come radio e TV via web) senza essere preventivamente autorizzati dal Responsabile;
5. usare la rete in modo difforme da quanto previsto dal presente documento e dalle leggi penali, civili e amministrative in materia di disciplina dell'attività e dei servizi svolti in rete;
6. scaricare software gratuiti senza aver verificato il rispetto delle condizioni di licenza e la sicurezza del download;
7. partecipare a forum e/o utilizzare chat se non per motivi strettamente attinenti l'attività lavorativa.

Relativamente all'utilizzo dei singoli PC affidati agli utenti, si precisa che l'assegnazione delle risorse non ne comporta la privatezza, in quanto trattasi di strumenti di esclusiva proprietà scolastica e quindi i files memorizzati non sono né tutelati né garantiti dall'Istituto per qualsiasi causa.

7.1 USO DELLA POSTA ELETTRONICA

L'utilizzo del servizio di posta elettronica istituzionale è consentito solo per ragioni di servizio.

Tutti gli utenti dovranno valutare attentamente, prima di aprirli, i messaggi che provengono sulla propria casella di posta elettronica, in caso di mail di dubbia provenienza, gli allegati non dovranno essere aperti.

Al dipendente non è consentito:

1. utilizzare la posta elettronica istituzionale per motivi non attinenti alle mansioni assegnate;
2. utilizzare l'indirizzo di posta elettronica istituzionale per la partecipazione a dibattiti, forum e mail-list, salvo specifica autorizzazione in tal senso da parte del responsabile;
3. aprire gli allegati di non comprovata origine in assenza di software antivirus aggiornato sulla propria postazione di lavoro;
4. effettuare chiamate a link contenuti all'interno di messaggi a meno di comprovata sicurezza sul contenuto dei siti richiamati;
5. rispondere ad e-mail pervenute da mittenti sconosciuti. Nel dubbio si suggerisce di cancellarle preventivamente;
6. utilizzare il servizio di posta per inoltrare giochi, scherzi, barzellette, appelli e petizioni e altre e-mail che non siano di lavoro;
7. allegare al testo delle comunicazioni materiale insicuro o files di dimensioni eccessive;
8. prestare particolare attenzione ai messaggi di phishing, ossia messaggi di posta contenenti link a siti che mirano ad estorcere le credenziali di accesso ai sistemi informatici.

7.2 CONTROLLI

Qualora le misure tecniche preventive non fossero sufficienti ad evitare le anomalie, gli eventi dannosi o le situazioni di pericoli che possono verificarsi, l'Istituto può avvalersi di un sistema di controllo a distanza per verificare, nel rispetto dei principi di pertinenza e non eccedenza (paragrafo 5 del Provvedimento del Garante), ogni qualsivoglia situazione anomala.

7.3 PROVVEDIMENTI DISCIPLINARI

La contravvenzione al presente disciplinare comporta la revoca delle autorizzazioni ad accedere alle risorse informatiche fatte salve le più gravi sanzioni previste dalle norme vigenti civili e penali.

Eventuale interruzione del servizio scatta nei seguenti casi:

1. quando non sussiste più la condizione di dipendente o collaboratore autorizzato o non è confermata l'autorizzazione all'uso;
2. quando è accertato un uso non corretto del servizio da parte dell'utente o comunque un uso estraneo ai suoi compiti professionali;

3. in caso di diffusione o comunicazioni imputabili direttamente o indirettamente all'utente di password, procedure di connessione, indirizzi IP ed altre informazioni tecniche riservate;
4. in caso di concessione di accesso ad Internet diretta o indiretta a qualsiasi titolo da parte dell'utente a terzi;
5. In caso di accesso doloso dell'utente a Directory, a siti o file o servizi non rientranti fra quelli per lui autorizzati.

Al verificarsi di uno qualsiasi dei casi sopra elencati il D.S. provvederà ad attivare la procedura per i provvedimenti disciplinari, come previsto dalla vigente normativa.

Per anomalie ancor più gravi riscontrate l'istituto provvederà a segnalare l'abuso alla Autorità competente.

8. Tutela della privacy

8.1 TUTELA DELLA PRIVACY: GARANZIE GENERALI

Tutte le operazioni relative all'uso della rete sono improntate alla tutela della privacy.

La titolarità del trattamento dei dati personali è esercitata dal Dirigente Scolastico. Il Dirigente scolastico designa il responsabile del trattamento dei dati nella persona del D.SS.GG.AA.

Per l'attività amministrativa sono state adottate le misure minime, secondo quanto previsto dal D.P.R.318/1999: password, codice identificativo personale per ogni utente; programmi antivirus; protezione (firewall) e regolamentazione degli accessi ai locali che ospitano i dati riservati o in cui si trovano le postazioni di lavoro; criteri per garantire l'integrità e la trasmissione sicura dei dati.

Il database non è accessibile dall'esterno: le informazioni gestite non sono fisicamente accessibili dall'esterno, ovvero la loro fruizione è possibile solo dall'interfaccia utente del programma alla quale possono collegarsi solo utenti registrati. Non esistono parti non sottoposte a criteri di sicurezza, l'unico punto di accesso al sistema è la maschera iniziale che richiede l'inserimento di username e password.

Più utenti possono accedere al sistema contemporaneamente, ma ciascuno opererà in una propria sessione di lavoro indipendente dalle altre. L'utilizzo del registro elettronico da parte dei Docenti, comporta l'integrale applicazione del presente regolamento.

8.2 TUTELA DELLA PRIVACY: NORME CONCERNENTI IL PERSONALE DELLA SCUOLA

I voti del professore sono privati e consultabili solo dai genitori o dai docenti del Consiglio di classe di appartenenza.

Ogni docente per entrare nella piattaforma (registro elettronico) deve obbligatoriamente inserire i suoi personali username e password;

Non possono essere presenti due utenti con la stessa username

E' assolutamente vietato cedere password, ovvero consentire ad altri soggetti di effettuare operazioni in nome e per conto del titolare di una password.

Nell'ipotesi di conoscenza accidentale di dati e/o informazioni riguardanti altri soggetti (alunni, famiglie, docenti e altro personale o non della scuola) è assolutamente vietata la divulgazione, pubblicazione o qualsiasi altra operazione. La mancata osservanza di tali disposizioni darà luogo alle sanzioni previste per legge.

8.3 TUTELA DELLA PRIVACY: NORME CONCERNENTI FAMIGLIE, ALUNNI E STUDENTI

Alunni, studenti e famiglie possono consultare solo voti e informazioni riguardanti il soggetto interessato.

Ogni alunno, studente o genitore per entrare nel sistema deve obbligatoriamente inserire i suoi personali username e password;

Non possono essere presenti due utenti con la stessa username

E' assolutamente vietato cedere password, ovvero consentire ad altri soggetti di effettuare operazioni in nome e per conto del titolare di una password.

Nell'ipotesi di conoscenza accidentale di dati e/o informazioni riguardanti altri soggetti (alunni, famiglie, docenti e altro personale o non della scuola) è assolutamente vietata la divulgazione, pubblicazione o qualsiasi altra operazione. La mancata osservanza di tali disposizioni darà luogo alle sanzioni previste per legge

9. Informativa e trattamento dei dati

9.1 GENERALITÀ: INFORMATIVA E TRATTAMENTO DEI DATI PERSONALI AI SENSI DELL'ART. 13 DEL D.L. 30/06/2003 N. 196

Ai sensi di quanto previsto dalla normativa vigente questo Istituto è titolare del trattamento dei dati personali.

Le finalità e modalità del trattamento dei dati sono:

1. il trattamento viene effettuato ad opera di soggetti appositamente incaricati, che si avvarranno di strumenti elettronici e non, configurati in modo da garantire la riservatezza dei dati e nel rispetto del segreto professionale;
2. i dati potranno essere utilizzati per circolari e corrispondenza nell'ambito dell'attività istituzionale dell'Istituto;
3. il trattamento cessa nel momento in cui termina la permanenza dello studente a scuola;
4. il trattamento dei dati è obbligatorio per legge quando è indispensabile per adempiere alle finalità istituzionali della scuola;
5. le conseguenze di un esplicito rifiuto al trattamento comporteranno l'impossibilità da parte della scuola di impiegare il registro elettronico;
6. i dati personali non saranno oggetto di diffusione e saranno a conoscenza solo del personale responsabile e incaricato al trattamento

9.2 INFORMATIVA E TRATTAMENTO DEI DATI PERSONALI AI SENSI DELL'ART. 7 DEL D.L. 30/06/2003 N. 196

L'interessato ha diritto di ottenere la conferma dell'esistenza o meno di dati personali che lo riguardano, anche se non ancora registrati, e la loro comunicazione in forma intelligibile.

L'interessato ha diritto di ottenere l'indicazione:

1. dell'origine dei dati personali;
2. delle finalità e modalità del trattamento;
3. della logica applicata in caso di trattamento effettuato con l'ausilio di strumenti elettronici;
4. degli estremi identificativi del titolare, dei responsabili e del rappresentante designato ai sensi dell'articolo 5, comma 2;

5. dei soggetti o delle categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di rappresentante designato nel territorio dello Stato, di responsabili o incaricati.

9.3 L'INTERESSATO HA DIRITTO DI OTTENERE:

1. l'aggiornamento, la rettificazione ovvero, quando vi ha interesse, l'integrazione dei dati;
2. la cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge, compresi quelli di cui non è necessaria la conservazione in relazione agli scopi per i quali i dati sono stati raccolti o successivamente trattati;
3. l'attestazione che le operazioni di cui alle lettere a) e b) sono state portate a conoscenza, anche per quanto riguarda il loro contenuto, di coloro ai quali i dati sono stati comunicati o diffusi, eccettuato il caso in cui tale adempimento si rivela impossibile o comporta un impiego di mezzi manifestamente sproporzionato rispetto al diritto tutelato.

9.4 L'INTERESSATO HA DIRITTO DI OPPORSI, IN TUTTO O IN PARTE, PER MOTIVI LEGITTIMI:

1. al trattamento dei dati personali che lo riguardano, ancorché pertinenti allo scopo della raccolta;
2. al trattamento di dati personali che lo riguardano a fini di invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale.