Istituto Statale D'Arte " O. Licini " Ascoli Piceno
via III ottobre 18/a Tel. 0736 – 43902 fax 0736 – 43821
C.F.: 80008490445
E-mail : apsd01000a@istruzione.it

Misure organizzative adottate dall'Istituzione scolastica in materia di

TRATTAMENTO E GESTIONE DEI DATI PERSONALI

Articolo 1

Oggetto e ambito di applicazione

1. Il presente regolamento disciplina le modalità di trattamento dei dati personali, in formato cartaceo e elettronico, da parte dell'Istituzione Scolastica
2. Per dato personale si intende qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale;
3. Per dato sensibile si intende qualsiasi dato personale idoneo a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale;
4. Per dato giudiziario si intende qualsiasi dato personale idoneo a rivelare provvedimenti di cui all'articolo 3, comma 1, lettere da a) a o) e da r) a u), del D.P.R. 14 novembre 2002, n. 313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale.

Articolo 2

Principi di carattere generale

1. I trattamenti di dati personali effettuati all'interno dell'Istituzione Scolastica devono avvenire secondo le modalità definite dalla normativa in vigore, con particolare riguardo a quanto disposto dal Dlgs 196/2003 e dalla normativa collegata;
2. Occorre custodire e controllare i dati personali oggetto del trattamento per contenere nella misura più ampia possibile il rischio che i dati siano distrutti, dispersi anche accidentalmente, conoscibili fuori dai casi consentiti o altrimenti trattati in modo illecito;
3. Chiunque, all'interno di questa istituzione scolastica, tratti dati personali, è tenuto all'obbligo della dovuta riservatezza in ordine alle informazioni delle quali sia venuto a conoscenza;

4. L'obbligo di mantenere la dovuta riservatezza, in ordine alle informazioni delle quali si sia venuti a conoscenza nel corso dell'incarico, permane anche quando sia venuto meno l'incarico stesso;
5. Tutti i trattamenti dei dati personali vanno necessariamente organizzati secondo una procedura che garantisca: una continua e idonea custodia dei dati oggetto del trattamento; un adeguato controllo sugli accessi non autorizzati ai dati; il maggior livello possibile di sicurezza in merito alla conservazione dei dati;
6. Il trattamento dei dati personali è consentito soltanto per lo svolgimento delle funzioni istituzionali della scuola. Al di fuori delle finalità strettamente istituzionali, dentro la scuola non si possono trattare dati personali né su supporto cartaceo né su supporto elettronico;
7. I dati personali oggetto dei trattamenti devono essere esatti ed aggiornati, inoltre devono essere pertinenti rispetto alle finalità del trattamento, completi e non eccedenti le finalità per le quali vengono raccolti e trattati. Ne consegue che i trattamenti dei dati vanno ridotti a quanto indispensabile rispetto alle finalità istituzionali perseguite;
8. Nell'ambito delle indicazioni del presente Regolamento, particolare attenzione va prestata al trattamento di dati sensibili e giudiziari;
9. L'istituto esegue verifiche periodiche sull'attualità degli incarichi affidati in merito al trattamento dei dati, nonché sull'esattezza e l'aggiornamento dei dati sensibili e giudiziari, sulla loro pertinenza, completezza, non eccedenza e indispensabilità rispetto alle finalità perseguite.

Articolo 3

Accesso ai luoghi in cui si effettuano i trattamenti

1. L'accesso ai locali in cui si trovano le apparecchiature informatiche dell'istituzione scolastica (server di rete, computer, stampanti, ecc) utilizzati per il trattamento dei dati personali, nonché gli archivi e i registri cartacei contenenti dati personali, è controllato dalla vigilanza dei collab.scolastici addetti alla portineria ed è permesso esclusivamente al personale debitamente incaricato e autorizzato;
2. I locali ad accesso controllato sono chiusi anche se presidiati. Dopo l'uscita dell'ultimo incaricato/addetto al trattamento dei dati i locali sono chiusi a chiave;
3. L'elenco delle persone autorizzate ad accedere ai locali di cui al presente articolo è periodicamente verificato dal responsabile del trattamento o da un suo delegato: sinteticamente tutto il personale amministrativo di segreteria e collab scolastici adetti alla pulizia dei locali;
4. Eventuali visitatori occasionali delle aree ad accesso controllato sono previamente autorizzati dal Responsabile del trattamento dei dati e accompagnati da un incaricato, che controllerà che i visitatori non accedano a dati in possesso dell'istituzione scolastica se non previamente autorizzati e incaricati;
5. L'ingresso in locali ad accesso controllato da parte di dipendenti o estranei per operazioni di pulizia o di manutenzione avviene solo in seguito ad apposita convenzione e/o lettera con istruzioni che disciplinino ambiti e modalità delle operazioni effettuabili.

Articolo 4

Raccolta, Comunicazione e diffusione dei dati

1. E' vietata ogni forma di diffusione e comunicazione dei dati personali a terzi soggetti, a meno che ciò non sia previsto da Legge o da Regolamento e autorizzato dal titolare del trattamento dei dati personali;
2. I dati idonei a rivelare lo stato di salute non possono essere diffusi;
3. Le comunicazioni di dati agli interessati (persone fisiche e giuridiche a cui afferiscono i dati personali) dovranno avvenire in forma riservata; se effettuate per iscritto dovranno essere consegnate in contenitori chiusi.

Articolo 5

Tenuta dei registri e degli archivi cartacei

1. I dati personali trattati attraverso supporto cartaceo possono essere trattati solo da personale debitamente incaricato e nel rispetto delle disposizioni contenute nelle lettere d'incarico e nel presente regolamento;
2. I registri di classe, contenenti dati personali, durante l'orario delle lezioni devono essere tenuti in classe sulla scrivania e affidati all'insegnante di turno. Al termine delle lezioni vengono depositati dall'insegnante dell'ultima ora di lezione nel locale di portineria e conservati in luogo sicuro dai collab.scolastici per essere riprelevati da un incaricato del trattamento all'inizio delle lezioni;
3. I certificati medici ricevuti vanno consegnati al più presto in Segreteria;
4. Durante l'orario di servizio il docente è responsabile della custodia e della conservazione dei registri personali e dei registri di valutazione attraverso cui sono trattati dati personali. Fuori dall'orario di servizio il registro viene conservato nella sala adiacente la biblioteca in apposito cassetto di utilizzo esclusivo del docente fornito di chiusura a chiave;
5. E' fatto divieto di fotocopiare/scannerizzare documenti contenenti dati sensibili senza l'autorizzazione del responsabile o del titolare del trattamento;
6. E' fatto divieto di esportare documenti o copie contenenti dati personali, all'esterno dell'Istituto, senza l'autorizzazione del titolare o del responsabile del trattamento; tale divieto si estende anche all'esportazione telematica;
7. I dati comuni sono custoditi separati dai dati sensibili in sottofascicoli chiusi con dicitura "riservato";
8. I documenti contenenti dati sensibili e giudiziari sono custoditi in armadi e/o cassetti chiusi a chiave.

Articolo 5

Trattamenti in formato elettronico – Principi generali

1. Le principali misure di sicurezza relative ai trattamenti di dati in formato elettronico sono indicate nel Documento Programmatico sulla Sicurezza della presente Istituzione Scolastica;

2. L'utilizzo dei Personal Computer e della Rete interna è permesso esclusivamente per lo svolgimento delle attività istituzionali della scuola. Al riguardo si ritiene opportuno ricordare, oltre alle disposizioni del codice disciplinare contenuto nei CCNL che dispone sanzioni in caso di *"negligenza nella cura dei locali e dei beni mobili o strumenti a lui affidati o sui quali, in relazione alle sue responibilità, debba espletare azione di vigilanza"* anche l'art. 10, comma 3 del codice di comportamento quando dispone che *"il dipendente non utilizza a fini privati materiale ed attrezzature di cui dispone per ragioni di ufficio"* ;
3. La scuola adotta procedure per la custodia di copie di sicurezza, il ripristino della disponibilità dei dati e dei sistemi;
4. I computer della Segreteria devono essere connessi ad un segmento della rete locale non visibile o raggiungibile da altri computer dell'istituto;
5. La stampa di documenti contenenti dati sensibili è effettuata su stampanti poste in locali ad accesso controllato o presidiate dall'incaricato.

Articolo 6

Trattamenti in formato elettronico – Regole operative

1. E' fatto divieto, agli utilizzatori di strumenti elettronici, di lasciare incustodito, o accessibile lo strumento elettronico stesso; in particolare, in caso di allontanamento anche temporaneo dal posto di lavoro, è vietato lasciare aperto il proprio sistema operativo con la password inserita, a meno che il sistema non richieda automaticamente la password in caso di inattività prolungata;
2. L'accesso ai dati trattati elettronicamente da parte degli incaricati e degli addetti esterni alla manutenzione è possibile solo in seguito ad autorizzazione scritta;
3. La manutenzione degli elaboratori, che preveda o meno il trasferimento fisico presso un laboratorio di riparazioni, è autorizzata solo a condizione che il fornitore del servizio si impegni al rispetto della normativa sulla protezione dei dati personali; il fornitore si deve altresì impegnare a mantenere la dovuta riservatezza in ordine ai dati di cui sia venuto a conoscenza e a non utilizzarli fuori dai casi consentiti;
4. Tutte le operazioni di manutenzione che sono effettuate all'interno dell'Istituzione Scolastica avvengono con la supervisione del Responsabile del trattamento o di un suo delegato;
5. Gli hard disk non sono condivisi in rete se non in casi specifici e limitati;
6. E' fatto assoluto divieto di memorizzare, sulla propria postazione di lavoro, dati di carattere personale che non siano inerenti alla funzione svolta;
7. E' proibito installare qualsiasi programma da parte dell'utente o di altri operatori, a meno che non siano autorizzati dell'amministratore del sistema (se nominato) o dal Responsabile del trattamento;
8. E' vietato fare uso delle funzionalità di accesso remoto del proprio computer se non espressamente autorizzati dal Responsabile del trattamento o dell'amministratore del sistema (se nominato);
9. All'uso di supporti rimovibili (floppy, cd, zip) va sempre preferito l'utilizzo di internet o di un file server locale;
10. Va evitato l'uso di programmi shareware e di pubblico dominio se non se ne conosce la provenienza;

11. E' fatto 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 o l'amministratore del sistema (se nominato);
12. Va attivata la protezione massima per gli utenti del programmi di posta utilizzati, al fine di proteggersi dal codice html di certi messaggi e-mail, dato che alcune pagine web, per il solo fatto di essere visualizzate possono infettare il computer;
13. E' fatto divieto di utilizzare la posta elettronica inviando e ricevendo materiale che violi le leggi dello Stato;
14. Gli allegati di posta, se non si è certi della loro provenienza, non vanno aperti e in ogni caso vanno analizzati con un antivirus;
15. E' opportuno impostare l'antivirus anche nella funzione di autoriparazione;
16. Avvisare sempre l'amministratore di sistema nel caso in cui il processo di autoriparazione non vada a buon fine;
17. E' opportuno conservare le copie originali di tutti i programmi applicativi utilizzati e la copia di backup consentita per legge;
18. 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 anomalie di funzionamento quali ad esempio modifica e sparizione di dati, irregolarità nell'utilizzo del Computer.

Articolo 7

Disposizioni in merito alla gestione delle password

1. Tutti gli incaricati del trattamento dei dati personali accedono agli strumenti elettronici usati per i trattamenti attraverso un codice identificativo personale (in seguito indicato user-id) e password personale;
2. User-id e password iniziali sono assegnati dal Responsabile del sistema informativo D'Ortnzi Lorenzo della ditta Lorysoft di Folignano (AP);
3. I codici assegnati sono segreti, non possono essere assegnati né comunicati ad altri soggetti; vanno custoditi con diligenza e riservatezza;
4. L'user-id è costituita da 8 caratteri che corrispondono alle prime otto lettere del cognome ed eventualmente del nome;
5. La password è composta da almeno 8 caratteri alfanumerici. Detta password non contiene, né conterrà, elementi facilmente ricollegabili all'Istituzione scolastica, al suo utilizzatore o al suo ufficio;
6. La password deve essere autonomamente modificata dall'incaricato al primo accesso al sistema e dallo stesso consegnata in una busta chiusa al custode delle password, dsga Rita Carlini, la quale provvede a conservarle in un posto di difficile accesso;
7. Ogni sei mesi ciascun incaricato, con messaggio /avviso di scadenza, 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;
8. Le password verranno prontamente disattivate dopo tre mesi di non utilizzo;

9. In caso di necessità, l'amministratore di sistema (se nominato) è autorizzato a intervenire sui personal computer;
10. L'utente deve sostituire la password, nel caso ne accertasse la perdita o ne verificasse che altri non autorizzati ne sono venuti a conoscenza.

Articolo 8

Videosorveglianza

1. Il trattamento dei dati attraverso sistemi di videosorveglianza avviene secondo correttezza e per scopi determinati, espliciti e legittimi;
2. Sono fatti salvi i diritti dello studente alla riservatezza di cui all'art. 2 comma 2, del D.P.R. n.249/1998;
3. Le riprese effettuate, sono circoscritte a determinate aree circostanti tutto l'edificio scolastico ed attivate nell'orario di chiusura dell'istituto le riprese ogni 5 giorni vengono sovrascritte da altre;
4. L'accesso ai dati è permesso al titolare e al responsabile del trattamento dei dati personali;
5. Sono fornite alle persone che possono essere riprese, indicazioni chiare, anche se sintetiche, circa la presenza di impianti di videosorveglianza;
6. Il periodo di conservazione dei dati è limitato ai 5 gg. successivi alle riprese.

Articolo 8

Sanzioni

1. In caso di violazione delle disposizioni del presente regolamento, 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 dal regolamento d'istituto.