Ministero della Pubblica Istruzione
Istituto Comprensivo di Zelo Buon Persico
Via F.lli Cervi 1 – 26839 Zelo Buon Persico
Tel: 02 90659917 Fax: 02 91767620
C.F. 92503580158 – Cod. Mecc. LOIC805006
Sito: www.iczelobp.gov.it
e-mail: loic805006@istruzione.it , loic805006@pec.istruzione.it

Ai docenti
Agli Assistenti amm.vi
Ai Collaboratori scolastici
LORO SEDI

Il DIRIGENTE SCOLASTICO
in qualità di titolare del trattamento dati dell'Istituzione Scolastica

AI SENSI degli artt. 29 e 30 del "Codice in materia di protezione dei dati personali" (D. L.vo 96/03);
TENUTO CONTO del ruolo funzionale volto dalla S.V. nell'Istituzione Scolastica ai sensi degli artt. 22 e 34 del CCNL vigente nel Comparto Scuola;
CONSIDERATO che, nell'ambito di tale funzione, la S.V. compie operazioni di trattamento dei dati personali, nel rispetto delle norme previste in materia di trattamento dei dati personali;

DESIGNA INCARICATI DEL TRATTAMENTO DEI DATI

il personale docente e ATA, di ruolo o supplente, di volta in volta assegnato all'Istituzione e per gli ambiti per ognuno specificati.

UNITA' ORGANIZZATIVA	AMBITO DEI TRATTAMENTI
DOCENTI	Ogni dato inerente gli alunni e le rispettive famiglie limitatamente agli aspetti rilevanti e funzionali allo svolgimento della funzione docente ed educativa, nell'ambito delle attività previste dal PTOF. Dati relativi ad esperti e ditte esterne per quanto riguarda attività didattiche previste dal PTOF e incarichi organizzativi o funzionali all'offerta formativa dell'Istituzione deliberati dal collegio dei docenti o su espresso incarico o delega del Dirigente scolastico
ATA AMMINISTRATIVI	Alunni Dati personali Personale dipendente Dati personali Collaborazioni professionali – Dati personali Acquisti e fornitori – Dati personali Gestione finanziaria del Programma Annuale Gestione Istituzionale e Protocollo Dati di presenza
ATA COLLABORATORI	Accesso e trattamento dei dati personali in occasione della gestione delle comunicazioni telefoniche e a mezzo fax, della duplicazione attraverso fotocopie, del trasporto documenti e posta e del trasferimento fra i diversi uffici della scuola di domande, documenti ed elenchi contenenti dati personali e sensibili

Nello svolgimento di tale incarico la S.V. avrà accesso ai dati personali gestiti da questa istituzione scolastica e dovrà attenersi alle seguenti istruzioni specifiche, ai sensi dell'art. 11 del D. Leg.vo 196/2003:

1. effettuare il trattamento in modo lecito e secondo correttezza;
2. raccogliere e registrare i dati personali per scopi determinati, espliciti e legittimi, ed utilizzarli in altre operazioni del trattamento in termini compatibili con tali scopi;
3. verificare, ove possibile, l'esattezza dei dati e, se necessario, aggiornarli;
4. verificare che i dati siano pertinenti, completi e non eccedenti le finalità per le quali sono stati raccolti o successivamente trattati, secondo le indicazioni ricevute dal titolare / responsabile;
5. rispettare, nella conservazione, le misure di sicurezza predisposte dall'istituzione scolastica; in ogni operazione di trattamento deve essere garantita la massima riservatezza, anche tra incaricati non coinvolti nello specifico trattamento o pratica;
6. non portare documenti fuori dalla sede scolastica, neanche temporaneamente;
7. non fare copie della documentazione salvo autorizzazione del responsabile o del titolare;
8. durante il trattamento mantenere i documenti contenenti dati personali fuori dalla portata di terzi anche se dipendenti dell'istituzione;
9. al termine del trattamento custodire i documenti all'interno di archivi muniti di serratura o nei locali ad accesso vigilato;
10. 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;
11. nessun dato può essere comunicato a terzi o diffuso in qualsiasi forma, anche ad altri dipendenti non incaricati, senza la preventiva specifica autorizzazione del titolare o del responsabile;
12. le comunicazioni agli interessati, contenenti dati personali, dovranno avvenire in forma riservata; se effettuate per scritto dovranno essere consegnate direttamente all'interessato o in modo che non risultino accessibili i dati in esse contenute (foglio piegato e spillato o in busta chiusa);
13. 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;
14. informare prontamente il Titolare e il Responsabile del trattamento quando si verifichi la necessità di porre in essere operazioni di trattamento di dati personali per finalità o con modalità diverse da quelle risultanti dalle istruzioni riservate, nonché di ogni istanza di accesso ai dati personali da parte di soggetti interessati e di ogni circostanza che esuli dalle istruzioni impartite alle SS.VV;
15. non fornire telefonicamente o a mezzo fax dati e informazioni relativi a terzi, senza una specifica autorizzazione del Responsabile / Titolare;
16. non fornire telefonicamente o a mezzo fax dati e informazioni ai diretti interessati, senza avere la certezza della loro identità;
17. rispettare ed applicare le misure di sicurezza idonee a salvaguardare la riservatezza e l'integrità dei dati, indicate nelle allegate "Linee guida in materia di sicurezza" elaborate ai sensi dell'art. 31 del D.Lvo 196/2003;
18. seguire le attività di formazione organizzate dalla istituzione scolastica per gli incaricati del trattamento dati.

La presente designazione ha validità permanente e si intende conferita, di volta in volta, al personale inserito nell'ufficio o nella funzione anche in corso d'anno e viene comunque a cessare al modificarsi del rapporto di lavoro.
Tutto il personale incaricato è contrattualmente soggetto, anche al di fuori dell'orario di lavoro e anche dopo la cessazione del rapporto stesso, ad osservare il segreto professionale e a non divulgare quindi dati, fatti o informazioni di qualsiasi tipo di cui è venuto a conoscenza nello svolgimento dell'incarico conferito.

La presente designazione si intende automaticamente revocata alla data di cessazione del rapporto di lavoro con questa istituzione scolastica, per trasferimento ad altra istituzione o cessazione del rapporto di lavoro. Successivamente a tale data, la S.V. non sarà più autorizzata ad effettuare alcun tipo di trattamento di dati per conto di questa Istituzione Scolastica.

IL RESPONSABILE del TRATTAMENTO DATI
Il Dirigente Scolastico
Prof. Enrico Fasoli

LINEE GUIDA IN MATERIA DI SICUREZZA PER IL DOCENTE INCARICATO DEL TRATTAMENTO

Vengono di seguito indicate le misure operative da adottare per garantire la sicurezza dei dati personali.

1. Custodire in apposito armadio/cassetto dotato di serratura i seguenti strumenti/documenti:
    a. PC per accesso registro elettronico
    b. Certificazione medica riferita agli alunni
    c. Qualunque altro documento contenente dati personali o sensibili degli alunni
2. Verificare la corretta funzionalità dei meccanismi di chiusura dell'armadio/cassetto, segnalando tempestivamente al responsabile di sede eventuali anomalie.
3. Consegnare al collaboratore scolastico incaricato o portare personalmente il registro di classe nel luogo deputato alla sua custodia.
4. Seguire le istruzioni del docente responsabile dell'aula di informatica.
5. Consegnare in busta chiusa al responsabile di sede o al protocollo della sede centrale le comunicazioni riservate indirizzate agli uffici della sede centrale, ad altro personale della scuola e al dirigente scolastico

Per i docenti che utilizzano l'aula di informatica (nel caso di trattamento di dati personali) e per il responsabile dell'aula di informatica:

Seguire le seguenti istruzioni operative per l'utilizzo dei personal computers:

1. Non lasciare strumenti di archiviazione, cartelle o altri documenti a disposizione di estranei;
2. non consentire l'accesso ai dati a soggetti non autorizzati;
3. riporre i supporti in modo ordinato negli appositi contenitori e chiudere a chiave classificatori e armadi dove sono custoditi;
4. scegliere una password con le seguenti caratteristiche:
    a. originale
    b. composta da almeno otto caratteri
    c. che contenga almeno un numero
    d. 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
5. curare la conservazione della propria password ed evitare di comunicarla ad altri;
6. cambiare periodicamente (almeno una volta ogni tre mesi) la propria password;
7. modificare prontamente (ove possibile) la password assegnata dal custode delle credenziali;
8. trascrivere su un biglietto chiuso in busta sigillata e controfirmata la nuova password e consegnarla al custode delle credenziali;
9. spegnere correttamente il computer al termine di ogni sessione di lavoro;
10. non abbandonare la propria postazione di lavoro senza aver spento la postazione di lavoro o aver inserito uno screen saver con password;
11. comunicare tempestivamente al Titolare o al Responsabile qualunque "anomalia" riscontrata nel funzionamento del computer;
12. utilizzare le seguenti regole per la posta elettronica:
    a. non aprire documenti di cui non sia certa la provenienza
    b. non aprire direttamente gli allegati ma salvarli su disco e controllarne il contenuto con un antivirus

LINEE GUIDA IN MATERIA DI SICUREZZA PER L' ASSISTENTE AMMINISTRATIVO INCARICATO DEL TRATTAMENTO

1. Conservare sempre i dati del cui trattamento si è incaricati in apposito armadio assegnato, dotato di serratura;
2. accertarsi della corretta funzionalità dei meccanismi di chiusura dell'armadio, segnalando tempestivamente al Responsabile eventuali anomalie;
3. non consentire l'accesso alle aree in cui sono conservati dati personali su supporto cartaceo a estranei e a soggetti non autorizzati;

4. conservare i documenti ricevuti da genitori/studenti o dal personale in apposite cartelline non trasparenti;
5. consegnare al personale o ai genitori/studenti documentazione inserita in buste non trasparenti;
6. non consentire l'accesso a estranei al fax e alla stampante che contengano documenti non ancora ritirati dal personale;
7. effettuare esclusivamente copie fotostatiche di documenti per i quali si è autorizzati;
8. provvedere personalmente alla distruzione quando è necessario eliminare documenti inutilizzati;
9. non lasciare a disposizione di estranei fotocopie inutilizzate o incomplete di documenti che contengono dati personali o sensibili ma accertarsi che vengano sempre distrutte;
10. non abbandonare la postazione di lavoro per la pausa o altro motivo senza aver provveduto a custodire in luogo sicuro i documenti trattati;
11. segnalare tempestivamente al Responsabile la presenza di documenti incustoditi, provvedendo temporaneamente alla loro custodia;
12. attenersi alle direttive ricevute e non effettuare operazioni per le quali non si è stati espressamente autorizzati dal Responsabile o dal Titolare.

Riguardo ai trattamenti eseguiti con supporto informatico attenersi scrupolosamente alle seguenti indicazioni:

1. Non salvare file o cartelle contenenti dati sensibili sul desktop del PC; laddove ci fosse l'esigenza di tenere un file/cartella sul desktop è necessario salvarlo/a su disco rigido e poi inviarlo/a, tramite collegamento, al desktop;
2. Indicare, nel piè di pagina di ogni documento, il nome del file e del percorso, il nome del responsabile del procedimento e del responsabile della pratica (se diverso);
3. non lasciare dispositivi di archiviazione, cartelle o altri documenti a disposizione di estranei;
4. conservare i dati sensibili in armadi chiusi, ad accesso controllato o in files protetti da password;
5. non consentire l'accesso ai dati a soggetti non autorizzati;
6. riporre i supporti informatici in modo ordinato negli appositi contenitori e chiudere a chiave classificatori e armadi;
7. scegliere una password con le seguenti caratteristiche:
    a. originale
    b. composta da almeno otto caratteri
    c. che contenga almeno un numero
    d. 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
8. curare la conservazione della propria password ed evitare di comunicarla ad altri;
9. cambiare periodicamente (almeno una volta ogni tre mesi) la propria password;
10. modificare prontamente (ove possibile) la password assegnata dal custode delle credenziali;
11. trascrivere su un biglietto chiuso in busta sigillata e controfirmata la nuova password e consegnarla al custode delle credenziali;
12. spegnere correttamente il computer al termine di ogni sessione di lavoro;
13. non abbandonare la propria postazione di lavoro senza aver spento la postazione di lavoro o aver inserito uno screen saver con password;
14. comunicare tempestivamente al Titolare o al Responsabile qualunque "anomalia" riscontrata nel funzionamento del computer;
15. non riutilizzare i supporti informatici utilizzati per il trattamento di dati sensibili per altri trattamenti;
16. non gestire informazioni su più archivi ove non sia strettamente necessario e comunque curarne l'aggiornamento in modo organico;
17. utilizzare le seguenti regole per la posta elettronica:
    a. non aprire documenti di cui non sia certa la provenienza
    b. non aprire direttamente gli allegati ma salvarli su disco e controllarne il contenuto con un antivirus
    c. inviare messaggi di posta solo se espressamente autorizzati dal Responsabile
    d. controllare accuratamente l'indirizzo dei destinatario prima di inviare dati personali

LINEE GUIDA IN MATERIA DI SICUREZZA PER IL COLLABORATORE SCOLASTICO INCARICATO DEL TRATTAMENTO

1. Accertarsi che al termine delle lezioni non restino incustoditi i seguenti documenti, o dispositivi informatici che li contengono, segnalandone tempestivamente l'eventuale presenza al responsabile di sede e provvedendo temporaneamente alla loro custodia:
    a. Portatili per accesso registro elettronico
    b. Registro di classe
    c. Certificazione medica esibita dagli alunni a qualsiasi titolo
    d. Qualunque altro documento contenente dati personali o sensibili degli alunni o dei docenti
2. Accertarsi che al termine delle lezioni tutti i computer dell'aula di informatica siano spenti e che non siano stati lasciati incustoditi strumenti di archiviazione, cartelle o altri materiali, in caso contrario segnalarne tempestivamente la presenza al responsabile di laboratorio o di sede e provvedendo temporaneamente alla loro custodia. Non utilizzare i computer per scopi personali.
3. Verificare la corretta funzionalità dei meccanismi di chiusura di armadi che custodiscono dati personali, segnalando tempestivamente al responsabile di sede eventuali anomalie.
4. Procedere alla chiusura dell'edificio scolastico accertandosi che tutte le misure di protezione dei locali siano state attivate.

Per il collaboratore scolastico in servizio negli uffici di segreteria.

1. Effettuare esclusivamente copie fotostatiche di documenti per i quali si è autorizzati.
2. Non lasciare a disposizione di estranei fotocopie inutilizzate o incomplete di documenti che contengono dati personali o sensibili ma accertarsi che vengano sempre distrutte.
3. Non lasciare incustodito rubrica/quaderno contenenti gli indirizzi e i recapiti telefonici del personale e non annotarne il contenuto sui fogli di lavoro.
4. Non abbandonare la postazione di lavoro per la pausa o altro motivo senza aver provveduto a custodire in luogo sicuro i documenti trattati.
5. Non consentire che estranei possano accedere ai documenti dell'ufficio o leggere documenti contenenti dati personali o sensibili.
6. Segnalare tempestivamente al Responsabile del trattamento la presenza di documenti incustoditi e provvedere temporaneamente alla loro custodia.
7. Procedere alla chiusura dei locali non utilizzati in caso di assenza del personale.
8. Procedere alla chiusura dei locali di segreteria accertandosi che siano state attivate tutte le misure di protezione e che le chiavi delle stanze siano depositate negli appositi contenitori.
9. Attenersi alle direttive ricevute e non effettuare operazioni per le quali non si sia stati espressamente autorizzati dal Responsabile o dal Titolare.