

MANSIONARIO GENERALE

Il presente documento costituisce parte integrante dell'atto di designazione. Esso definisce istruzioni dettagliate sui trattamenti concessi. Al fine di rendere il presente adempimento il più efficace possibile, *si suggerisce di provvedere a contestualizzarlo alla singola scuola.*

MANSIONARIO DOCENTI

TIPI E MODI DI TRATTAMENTO CONCESSI

COMPLEMENTARI A QUELLI RIPORTATI NELL'ATTO DI DESIGNAZIONE

1. Relativamente ai PC della rete:

- archiviare i dati solo negli ambienti (solitamente cloud o server) a ciò dedicati
- non archiviare i dati sui pc della rete
- non trattare dati personali sui pc della rete della didattica se non in maniera strettamente indispensabile e nel rispetto di tutte le misure di sicurezza descritte nel **Sistema di Gestione per la Sicurezza delle Informazioni EUservice ("SGSI")**
- al termine di un'operazione che coinvolga il trattamento dei dati il docente dovrà cancellare i dati dal cestino, dalla cronologia e dalla funzione "download"

2. Relativamente alle password:

- le password di accesso ai PC della rete didattica vengono assegnate in via solo provvisoria da parte dell'Amministratore di sistema o dell'Assistente tecnico e cambiate dall'utente, che ne diventa il diretto responsabile, al primo utilizzo
- l'utente deve disconnettersi dalla sessione di lavoro al termine della propria attività, specie su device condiviso

3. Relativamente alle chiavette USB:

- La pen drive deve essere nuova o, comunque, formattata prima dell'uso, specie se si è in procinto di trasferire dati da un computer all'altro
- La pen drive, anche se utilizzata per trasferire dati, completato il passaggio deve necessariamente subire una formattazione con contestuale eliminazione di tutto il contenuto
- La pen drive non deve in nessun caso essere utilizzata come archivio di dati personali, nemmeno per breve tempo
- Il personale, in concomitanza con l'eventuale trasferimento di dati tramite pen drive, è tenuto a non perdere di vista tale chiavetta, mantenendone sempre il controllo, anche e soprattutto quando altro soggetto effettua operazioni di upload o download

4. Relativamente alle misure di protezione applicabili al registro elettronico:

- effettuare la disconnessione dal registro di classe in caso di interruzione della lezione anche laddove sia presente per default un sistema di disconnessione automatico

5. Relativamente alle comunicazioni:

- mantenere la riservatezza professionale come principio generale di condotta a tutela della privacy dello studente (D.P.R. n. 249/1998)
- la comunicazione degli avvisi in classe, soprattutto quelli afferenti a questioni sensibili, deve avvenire in maniera neutra e riservata. Mai fornire informazioni a terzi non destinatari delle stesse
- consegnare alla segreteria al termine dell'orario di lezione (e non lasciare in classe) eventuali documenti cartacei riguardanti questioni amministrative ritirati dagli alunni
- non costituire gruppi di classe WhatsApp, Telegram ed equivalenti, con gli studenti o con i genitori al fine di non incorrere in potenziali *data breach*
- non comunicare materiale didattico o effettuare comunicazioni relative alla didattica da e-mail personali private (diverse dall'e-mail istituzionale)
- utilizzare in via preferenziale il registro elettronico per le comunicazioni scuola-famiglia
- usare prudenza e buon senso nel gestire la corrispondenza prima di inviare una comunicazione contenente dati personali, privilegiando in ogni caso comunicazioni che rendono l'interessato il meno identificabile possibile

6. Relativamente alle foto e video:

- è vietato pubblicare sui propri canali social, foto o video o commenti relativi a fatti avvenuti nel corso delle attività didattiche o attività ad essere correlate
- ogni pubblicazione fatta sui propri profili social avviene sotto la responsabilità privata del docente e la scuola è esente da questa responsabilità



MANSIONARIO GENERALE

7. Relativamente alle **piattaforme didattiche**:

- riferire al Dirigente Scolastico, all'Animatore digitale e al DPO l'intenzione di utilizzare qualsiasi piattaforma didattica o servizio aggiuntivo al di fuori del registro elettronico, al fine di ottenere una autorizzazione espressa
- verificare l'identità degli autorizzati e dei partecipanti alle aule virtuali
- non far accedere alla piattaforma persone non autorizzate
- generare la riunione attraverso istruzioni impartite da parte dell'Animatore digitale e del team digitale
- seguire la procedura predisposta dal team digitale per l'archiviazione dei compiti in digitale

8. Relativamente al **PEI/PDP**:

- attenersi alle indicazioni fornite per l'elaborazione, la consultazione, l'archiviazione e comunicazione all'interessato del PEI/PDP fornite da parte dell'Istituto
- in caso di scambio di informazioni sui PEI/PDP tra docenti attraverso l'indirizzo mail istituzionale e/o i Drive, tutti i dati degli alunni dovranno essere resi il più anonimi possibile, al fine di minimizzare il rischio di utilizzo dei dati sensibili da parte di Google/Microsoft

9. Relativamente all'**utilizzo dei propri dispositivi personali utilizzati per la Didattica digitale integrata**:

- attenersi alla policy sul BYOD

10. Raccolta di informazione da moduli:

- Ogni questionario deve essere autorizzato dal DS
- in caso di ricezione di moduli provenienti da soggetti esterni alla scuola ed indirizzati agli alunni verificarne sempre i requisiti di legalità con il Dirigente Scolastico ed eventualmente il DPO

Per tutto quanto qui non indicato si rinvia all'atto di designazione e all'intero **Sistema di Gestione per la Sicurezza delle Informazioni EUservice ("SGSI")**



MANSONARIO SEGRETERIA

TIPI E MODI DI TRATTAMENTO CONCESSI

COMPLEMENTARI A QUELLI RIPORTATI NELL'ATTO DI DESIGNAZIONE

TIPI E MODI DI TRATTAMENTO CONCESSI

COMPLEMENTARI A QUELLI RIPORTATI NELL'ATTO DI DESIGNAZIONE

1. Relativamente ai PC della rete:

- archiviare i dati solo negli ambienti (solitamente cloud o server) a ciò dedicati
- non archiviare i dati sui pc della rete
- non trattare dati personali sui pc della rete della didattica se non in maniera strettamente indispensabile e nel rispetto di tutte le misure di sicurezza descritte nel **Sistema di Gestione per la Sicurezza delle Informazioni EUservice ("SGSI")**
- al termine di un'operazione che coinvolga il trattamento dei dati sarà necessario cancellare i dati dal cestino, dalla cronologia e dalla funzione "download"

2. Relativamente alle password:

- le password di accesso ai PC della rete di segreteria vengono assegnate in via solo provvisoria da parte dell'Amministratore di sistema o dell'Assistente tecnico e cambiate dall'utente, che ne diventa il diretto responsabile, al primo utilizzo
- l'utente deve disconnettersi dalla sessione di lavoro al termine della propria attività, specie su device condiviso

3. Relativamente alle chiavette USB (in forza delle misure minime di sicurezza ICT AGID per la PA):

- La pen drive deve essere nuova o, comunque, formattata prima dell'uso, specie se si è in procinto di trasferire dati da un computer all'altro
- La pen drive, anche se utilizzata per trasferire dati, completato il passaggio deve necessariamente subire una formattazione con contestuale eliminazione di tutto il contenuto
- La pen drive non deve in nessun caso essere utilizzata come archivio di dati personali, nemmeno per breve tempo
- Il personale, in concomitanza con l'eventuale trasferimento di dati tramite pen drive, è tenuto a non perdere di vista tale chiavetta, mantenendone sempre il controllo, anche e soprattutto quando altro soggetto effettua operazioni di upload o download

4. Relativamente alle comunicazioni:

- mantenere la riservatezza professionale come principio generale di condotta a tutela della privacy dello studente (DPR 249/1998) ed in generale di tutto il personale della scuola e di tutti gli interessati
- per le comunicazioni destinate a più destinatari deve essere utilizzato il campo CCN
- archiviare correttamente i documenti cartacei riguardanti questioni amministrative ritirati da parte del personale docente durante l'orario di lezione e quindi consegnati alla segreteria
- non costituire gruppi di classe WhatsApp, Telegram ed equivalenti, con gli studenti o con i genitori al fine di non incorrere in potenziali data breach
- effettuare le comunicazioni alle famiglie da indirizzo mail istituzionale
- usare prudenza e buon senso nel gestire la corrispondenza prima di inviare una comunicazione contenente dati personali, privilegiando in ogni caso comunicazioni che rendono l'interessato il meno identificabile possibile

5. Relativamente alle foto e video:

- è vietato pubblicare sui propri canali social, foto o video o commenti relativi a fatti avvenuti nel corso delle attività didattiche o attività ad essere correlate
- ogni pubblicazione fatta sui propri profili social avviene sotto la responsabilità privata del personale di segreteria e la scuola è esente da questa responsabilità

6. Relativamente al PEI/PDP:

- attenersi alle indicazioni fornite per l'elaborazione, la consultazione, l'archiviazione e comunicazione all'interessato del PEI/PDP fornite da parte dell'Istituto

7. Relativamente all'utilizzo dei propri dispositivi personali utilizzati per la Didattica digitale integrata:

- attenersi alla policy sul BYOD

8. Raccolta di informazione da moduli:



MANSIONARIO GENERALE

- Ogni questionario deve essere autorizzato dal DS
 - in caso di ricezione di moduli provenienti da soggetti esterni alla scuola ed indirizzati agli alunni verificarne sempre i requisiti di legalità con il Dirigente Scolastico ed eventualmente il DPO
- 9. Gestione Amministrazione trasparente e Albo on line:**
- identificare i corretti responsabili alla pubblicazione
 - non confondere le due sezioni e seguire le indicazioni riportate nella relativa policy
 - applicare correttamente l'oblio al termine del periodo di pubblicazione previsto per legge
- 10. Sistema di archiviazione dei documenti:**
- attenersi alle indicazioni fornite all'interno del Manuale della gestione documentale, del Titolare e Massimari di scarto

Per tutto quanto qui non indicato si rinvia all'atto di designazione e all'intero **Sistema di Gestione per la Sicurezza delle Informazioni EUservice ("SGSI")**



MANSIONARIO GENERALE

MANSIONARIO CS

TIPI E MODI DI TRATTAMENTO CONCESSI

COMPLEMENTARI A QUELLI RIPORTATI NELL'ATTO DI DESIGNAZIONE

1. **Relativamente ai PC della rete:**
 - archiviare i dati solo negli ambienti (solitamente cloud o server) a ciò dedicati
 - non archiviare i dati sui pc della rete della segreteria
 - non trattare dati personali sui pc della rete della didattica se non in maniera strettamente indispensabile e nel rispetto di tutte le misure di sicurezza descritte nel **Sistema di Gestione per la Sicurezza delle Informazioni EUservice ("SGSI")**
 - al termine di un'operazione che coinvolga il trattamento dei dati sarà necessario cancellare i dati dal cestino, dalla cronologia e dalla funzione "download"
2. **Relativamente alle password**
 - le password di accesso ai PC della rete di segreteria vengono assegnate in via solo provvisoria da parte dell'Amministratore di sistema o dell'Assistente tecnico e cambiate dall'utente, che ne diventa il diretto responsabile, al primo utilizzo
 - è necessario prevedere un cambio password periodico
 - l'utente deve disconnettersi dalla sessione di lavoro al termine della propria attività
11. **Relativamente alle chiavette USB (in forza delle misure minime di sicurezza ICT AGID per la PA):**
 - La pen drive deve essere nuova o, comunque, formattata prima dell'uso, specie se si è in procinto di trasferire dati da un computer all'altro
 - La pen drive, anche se utilizzata per trasferire dati, completato il passaggio deve necessariamente subire una formattazione con contestuale eliminazione di tutto il contenuto
 - La pen drive non deve in nessun caso essere utilizzata come archivio di dati personali, nemmeno per breve tempo;
 - Il personale, in concomitanza con l'eventuale trasferimento di dati tramite pen drive, è tenuto a non perdere di vista tale chiavetta, mantenendone sempre il controllo, anche e soprattutto quando altro soggetto effettua operazioni di upload o download
3. **Misure di protezione applicabili alle comunicazioni:**
 - mantenere la riservatezza professionale come principio generale di condotta a tutela della privacy dello studente (D.P.R. n. 249/1998) ed in generale di tutto il personale della scuola e di tutti gli interessati
 - non diffondere per nessuna ragione dati e informazioni della scuola all'esterno dell'organizzazione
 - non costituire gruppi di classe WhatsApp, Telegram, ed equivalenti, con gli studenti o con i genitori al fine di non incorrere in potenziali data breach
 - effettuare eventuali comunicazioni ai diretti interessati in maniera discreta evitando che altri interessati vengano a conoscenza di tali comunicazioni
4. **Conservazioni delle rubriche e di altri dati personali:**
 - archiviare le rubriche con i dati del personale della scuola in un cassetto chiuso a chiave
 - assicurarsi che persone esterne all'organizzazione non accedano in alcuna maniera ai dati trattati dallo stesso collaboratore scolastico
 - assicurarsi di distruggere eventuali dati raccolti su post-it al termine del turno di servizio
5. **Misure applicabili alle foto e video:**
 - è vietato pubblicare sui propri canali social, foto o video o commenti relativi a fatti avvenuti nel corso delle attività didattiche o attività ad essere correlate
 - ogni pubblicazione fatta sui propri profili social avviene sotto la responsabilità privata del personale di segreteria e la scuola è esente da questa responsabilità
6. **Misure di protezione applicabili all'utilizzo dei propri dispositivi personali utilizzati per la Didattica digitale integrata:**
 - attenersi alla policy sul BYOD
7. **Gestione delle chiavi della struttura:**
 - conservare le chiavi della scuola in luoghi sicuri e chiusi a chiave, non visualizzabili dagli esterni dell'organizzazione



MANSIONARIO GENERALE

Per tutto quanto qui non indicato si rinvia all'atto di designazione e all'intero **Sistema di Gestione per la Sicurezza delle Informazioni EUservice ("SGSI")**

Copyright 2022

EUSERVICE s.r.l. - via Dante Alighieri, 12 - 00027 Roviano (RM) - P.IVA 08879271008



[Questo opera è distribuita con Licenza Creative Commons Attribuzione - Non commerciale - Non opere derivate 4.0 Internazionale](https://creativecommons.org/licenses/by-nc-nd/4.0/)



ELENCO ARCHIVI ACCESSIBILI

Poste le regole di cui sopra, nel presente paragrafo il personale troverà l'elenco degli archivi a cui è consentito l'accesso in base alle proprie funzioni.

Dirigente Scolastico

Archivi didattici:

Tutti gli archivi degli insegnanti (su tutto l'istituto) e inoltre:
fascicoli amministrativi.

Archivi del personale:

fascicolo docenti (CV, corsi, valutazione, etc.)
curriculum vitae personale ATA.

Altri archivi:

archivi Legge 81 (infortuni)
archivi HACCP (formazione)

Insegnante

Archivi didattici:

registro elettronico, per le classi a lui assegnate
mail istituzionale
fascicoli didattici degli allievi a lui assegnati (siano essi cartacei o informatici)
valutazioni degli allievi a lui assegnati (siano esse cartacee o informatiche)
verbali Consigli di classe per le classi lui assegnate
verbali Collegio docenti
documentazione relativa a PEI, disturbi alimentari, patologie e tutti gli archivi previsti per legge.

Animatore digitale

Repository

Segreteria

Archivi didattici:

registri di classe
fascicoli didattici degli allievi (siano essi cartacei o informatici)
valutazioni degli allievi (siano esse cartacee o informatiche)
verbali consigli di classe
verbali collegio docenti.

Altri archivi:

fascicoli amministrativi del personale (siano essi cartacei o informatici)
fascicoli amministrativi degli allievi (siano essi cartacei o informatici)
fascicoli fornitori

