



*Ministero dell'Istruzione, dell'Università e della Ricerca*  
*Ufficio Scolastico Regionale per il Veneto*  
**UFFICIO VII - AMBITO TERRITORIALE DI VERONA**  
 Viale Caduti del Lavoro, 3 – 37124 Verona

Verona, 17/02/2016

**Oggetto: Individuazione degli “Incaricati del trattamento dei dati personali” ai sensi dell’art. 30 del D.Lgs. n.196/2003.**

### Il Dirigente

**Visto** Il Codice in materia di protezione dei dati personali, di cui al D.Lgs. n.196 del 30 giugno 2003 e s.m. e il relativo Disciplinare tecnico in materia di misure di sicurezza, Allegato B;

**Visto** Il D.P.R. 7 gennaio 2006, n. 305, recante il Regolamento per l’identificazione dei dati sensibili e giudiziari e delle relative operazioni effettuate dal M.I.U.R.;

**Considerato** che l’Ufficio Scolastico Regionale per il Veneto, in persona del Direttore Generale pro tempore, è titolare del trattamento dei dati personali, sensibili e giudiziari contenuti nelle banche dati, automatizzate o cartacee, presenti presso le proprie strutture, e che gli stessi vengono trattati per il perseguimento dei fini istituzionali del medesimo Ufficio Scolastico Regionale;

**Visto** il D.Lgs. 30 marzo 2001, n. 165, e s.m.;

**Vista** la Delibera del Garante per la protezione dei dati personali del 14 giugno 2007, recante “Linee guida in materia di trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro in ambito pubblico”, pubblicata in G.U. 13 luglio 2007, n.161;

**Preso atto** del Documento Programmatico per la sicurezza prot. n. 4371 / A10b del 30 marzo 2011, a firma del Dirigente pro tempore dell’Ufficio Scolastico Provinciale di Verona;

**Visto** il provvedimento del Direttore Generale U.S.R. Veneto, prot. AOODRVE 5980 del 18 maggio 2015, con il quale sono stati individuati, a seguito della riorganizzazione dell’Ufficio Scolastico Regionale per il Veneto di cui al D.P.C.M. 11 febbraio 2014, n. 98 e al Decreto Ministeriale prot. n. 925 del 18 dicembre 2014, i Responsabili del trattamento dei dati personali, sensibili e giudiziari che l’Ufficio Scolastico Regionale per il Veneto deve acquisire e trattare per le proprie finalità istituzionali;

**Visto** il successivo provvedimento dell’Ufficio Scolastico Regionale per il Veneto, prot. A00DRVE n. 824 del 13 gennaio 2016, nel quale si ravvisa la necessità di rinnovare/aggiornare il precedente provvedimento n.5980 del 18 maggio 2015 cit., a seguito dei mutamenti intervenuti nell’ambito del personale in servizio presso l’U.S.R. Veneto e presso i sette Uffici - Ambiti territoriali;

**Considerato** che il predetto provvedimento designa quale “Responsabile del trattamento dei dati trattati dall’Ufficio VII (Ufficio Ambito territoriale per la provincia di Verona)” il sottoscritto nella qualità di Dirigente;

**Considerato** che le operazioni di trattamento possono essere effettuate solo da Incaricati che operano sotto la diretta autorità del titolare o del responsabile, attenendosi alle istruzioni impartite;



*Ministero dell'Istruzione, dell'Università e della Ricerca*  
*Ufficio Scolastico Regionale per il Veneto*  
**UFFICIO VII - AMBITO TERRITORIALE DI VERONA**  
*Viale Caduti del Lavoro, 3 – 37124 Verona*

Per quanto sopra premesso, il sottoscritto, in qualità di Responsabile del trattamento dei dati,

### INDIVIDUA

quale **“Incaricato del trattamento dei dati personali”** il seguente personale dell'Ambito Territoriale di Verona:

**Ufficio del Dirigente:** unità operative che collaborano direttamente con lo Scrivente: Maura Bellamoli, Roberta Isoli, Angela Capuzzo, Luciana De Corso, Egidio Cavallini, Giuseppe Nicotra, Zenone Giovanni, Roberto Grison, Michele Bonetti, Giuliana Guadagnini, Laura Parenti, Giorgia Nani, Annalisa Tiberio, Cinzia Maggi;

**Ufficio I – Affari generali e contabilità,** Coord. Francesco Lo Duca, Unità oper.: Chiara Anselmi, Clara Baratta, Alda Ferrari, Simonetta De Santis, Michele Sivero, Carlo Rubino, Alberto Failla, Anna Maria Cortese, Isabella Palombi, Cristina Sacchetto, Fiorenzo Bianchi, Raffaele Maietta, Grazia Baccaro.

**Ufficio II – Comunicazione,** Coord. Raffaele Leto, Unità oper.: Leda Sartori, Ivana Nuvoloni, Fabio Barba;

**Ufficio III – Affari Legali,** Coord. Dario Lo Guarro, Unità oper.: Elisabetta Bonato, Domenico Ciuffreda, Silvana Girardi, Patrizia Panarotto;

**Ufficio IV – Reclutamento,** Coord. Annamaria Chiavenato, Unità oper.: Celeste Lupo, Valeria Tosi, Mariella Turri;

**Ufficio V – Organici di tutti gli ordini e gradi di scuola – Esami di stato di 1° e 2° grado,** Coord. Valeria Giustizieri, Unità oper.: Luca Ciuffreda, Giulia Guerra, Orietta Perina;

**Ufficio VI – Gestione del personale scolastico,** Coord. Mariachiara Merli, Unità oper.: Rita Loredana Bertucco, Donatella De Martino, Maria Cristina Pettenella, Donatella Rizzi;

**Ufficio VII – Personale A.T.A.,** Coord. Giovanni Salzani, Unità oper.: Marcella Padovini, Sonia Spada;

**Ufficio VIII – Unità complessa per l'Ufficio procedimenti disciplinari ed i trattamenti di quiescenza,** Coord: Maria Donata Padovani, Unità oper.: Lorella Bellorio, Patrizia Luly;

**Ufficio IX – Archivio,** Coord: Carlo Rubino, Unità oper: Giuliano Marchioro, Patrizia Muletto, Armando Bolan.

Per ragioni organizzative, alcune unità operative potranno essere utilizzate a supporto di altri uffici.

A ciascun incaricato verrà data notifica delle istruzioni (All. 1), costituenti le misure minime di sicurezza di cui agli art. 33 e ss. D.Lgs. 196/2003, alle quali gli stessi si devono attenere.

Gli incaricati devono attenersi altresì all'osservanza delle “Linee guida in materia di trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro in ambito pubblico”, che sono consultabili sul sito del Garante per la protezione dei dati personali.

In coerenza con quanto disposto dal provv. prot. A00DRVE n. 824 del 13 gennaio 2016 richiamato in premessa, gli incaricati sono altresì tenuti ad eseguire il trattamento dei dati personali, sensibili e giudiziari che gestiscono nell'espletamento dei propri compiti, come da organigramma funzionale di quest'Ufficio, **esclusivamente all'interno delle rispettive stanze, nonché negli archivi**, ubicati nella sede di servizio di Verona, Viale Caduti del lavoro n. 3, nei quali devono custodire la relativa documentazione.



*Ministero dell'Istruzione, dell'Università e della Ricerca*  
*Ufficio Scolastico Regionale per il Veneto*  
**UFFICIO VII - AMBITO TERRITORIALE DI VERONA**

*Viale Caduti del Lavoro, 3 - 37124 Verona*

Gli incaricati debbono inoltre osservare il divieto di trattare i dati personali degli alunni frequentanti le scuole di ogni ordine e grado al di fuori degli adempimenti prescritti da norme di legge o di regolamento.

Il presente provvedimento con le istruzioni di cui all'allegato 1, costituenti le misure minime di sicurezza di cui agli art. 33 e ss. del D.lgs.196/2003, sono pubblicati sul sito istituzionale: [www.istruzioneverona.it](http://www.istruzioneverona.it), area Amministrazione trasparente – Provvedimenti – Provvedimenti del Dirigente.

**IL DIRIGENTE**

*Stefano Quaglia*

firma autografa sostituita a mezzo stampa  
(art.3, comma 2, D. Lgs. n.39 del 1993)

Il Responsabile del procedimento  
*Dott.ssa Mariachiara Merli*



*Ministero dell'Istruzione, dell'Università e della Ricerca*  
*Ufficio Scolastico Regionale per il Veneto*  
**UFFICIO VII - AMBITO TERRITORIALE DI VERONA**  
*Viale Caduti del Lavoro, 3 – 37124 Verona*

Allegato 1

ISTRUZIONI ALL'INCARICATO DEL TRATTAMENTO DEI DATI PERSONALI, SENSIBILI E/O GIUDIZIARI.

In ottemperanza alle disposizioni del Codice in materia di protezione dei dati personali (D.Lgs n. 196 del 30 giugno 2003 e s.m.), al disciplinare tecnico di cui all'All. B del D.Lgs n. 196 del 30 giugno 2003, al Documento Programmatico per la sicurezza dell'Ufficio Scolastico Regionale per il Veneto, ed in relazione alle attività svolte nell'ambito dell'Ufficio di appartenenza, l'Incaricato dovrà effettuare i trattamenti di dati personali di propria competenza, attenendosi scrupolosamente alle seguenti istruzioni ed ad ogni ulteriore indicazione, anche verbale, che potrà essere fornita dal Responsabile del trattamento.

I dati personali devono essere trattati:

- a) in osservanza al criterio di pertinenza della raccolta, dell'utilizzo, dell'elaborazione della comunicazione nella misura minima indispensabile e non eccedente alla finalità istituzionale prevista da una norma di legge o di regolamento;
- b) in osservanza dei criteri di riservatezza, nel rispetto dei diritti e delle libertà fondamentali e della dignità dell'interessato;
- c) in modo lecito e secondo correttezza;
- d) per un periodo di tempo non superiore a quello necessario agli scopi per i quali i dati sono stati raccolti o successivamente trattati;
- e) nel pieno rispetto delle misure minime di sicurezza, custodendo e controllando i dati oggetto di trattamento in modo da evitare i rischi, anche accidentali, di distruzione o perdita, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.
- f) con l'obbligo di informare il Responsabile in caso di incidenti relativi alla sicurezza dei dati.

Le misure minime di sicurezza (di cui agli artt. 33 – 36 e di cui all'allegato B del citato D.lgs.196/2003) sono obbligatorie e sono distinte in funzione delle seguenti modalità di trattamento dei dati:

- 1. Senza l'ausilio di strumenti elettronici** (es. dati in archivi cartacei o su supporto magnetico/ottico);
- 2. Con strumenti elettronici** (PC ed elaboratori).

## **1. TRATTAMENTI SENZA L'AUSILIO DI STRUMENTI ELETTRONICI**

Le misure di sicurezza applicate alle copie o alle riproduzioni, il cui numero deve in ogni caso essere limitato all'effettiva necessità, dei documenti contenenti dati personali devono essere identiche a quelle applicate agli originali.

### **1.1 Custodia**

- I documenti contenenti dati personali devono essere custoditi in modo da non essere accessibili a persone non incaricate del trattamento (es. armadi o cassette chiusi a chiave).
- I documenti contenenti dati personali che vengono prelevati dagli archivi per l'attività quotidiana devono esservi riposti a fine giornata.
- I documenti contenenti dati personali non devono rimanere incustoditi su scrivanie o tavoli di lavoro.

### **1.2 Comunicazione**

- L'utilizzo dei dati personali deve avvenire in base al "principio di necessità" e cioè essi non devono essere condivisi, comunicati o inviati a persone che non ne necessitano per lo svolgimento delle proprie mansioni lavorative (anche se queste persone sono a loro volta incaricate del trattamento). I dati non devono essere comunicati all'esterno dell'Ufficio e comunque a soggetti terzi, se non previa autorizzazione del Responsabile.

### **1.3 Distruzione**

- Qualora sia necessario distruggere le copie o le riproduzioni di documenti contenenti dati personali, questi devono essere distrutti utilizzando gli appositi apparecchi "distruggi documenti" o, in assenza, devono essere sminuzzati in modo da non essere più ricomponibili.



Ministero dell'Istruzione, dell'Università e della Ricerca  
Ufficio Scolastico Regionale per il Veneto  
**UFFICIO VII - AMBITO TERRITORIALE DI VERONA**

Viale Caduti del Lavoro, 3 – 37124 Verona

- I supporti magnetici od ottici contenenti dati personali devono essere cancellati prima di essere riutilizzati. Se ciò non è possibile, essi devono essere distrutti.

**1.4 Ulteriori istruzioni in caso di trattamento di dati sensibili e/o giudiziari.**

- È sempre vietata la diffusione di dati sensibili o giudiziari.
- I documenti contenenti dati sensibili e/o giudiziari devono essere controllati e custoditi dagli Incaricati in modo che non vi accedano persone prive di autorizzazione. Ad esempio, la consultazione di documenti/certificati per l'inserimento in procedure informatiche di gestione/amministrazione del personale di dati relativi a permessi sindacali, assenze per malattie, certificati di handicap, ecc., deve avvenire per il tempo strettamente necessario alla digitazione stessa e, subito dopo, i documenti devono essere archiviati in base alle presenti istruzioni.
- L'archiviazione dei documenti cartacei contenenti dati sensibili e/o giudiziari deve avvenire in locali ad accesso controllato, utilizzando armadi o cassette chiuse a chiave.
- Per accedere agli archivi contenenti dati sensibili e/o giudiziari fuori orario di lavoro è necessario ottenere una preventiva autorizzazione da parte del Responsabile oppure farsi identificare e registrare su appositi registri.

**2. TRATTAMENTI CON STRUMENTI ELETTRONICI**

**2.1 Gestione delle credenziali di autenticazione**

- La legge prevede che l'accesso alle procedure informatiche che trattano dati personali sia consentito agli Incaricati in possesso di "credenziali di autenticazione" che permettano il superamento di una procedura di autenticazione. Le credenziali di autenticazione consistono in un codice per l'identificazione dell'Incaricato (*user-id*), associato ad una parola chiave riservata (*password*), oppure in un dispositivo di autenticazione (es. *smart card*). Gli Incaricati devono utilizzare e gestire le proprie credenziali di autenticazione attenendosi alle seguenti istruzioni:
- Le *user-id* individuali per l'accesso alle applicazioni non devono mai essere condivise tra più utenti (anche se Incaricati del trattamento). Nel caso altri utenti debbano poter accedere ai dati è necessario richiedere l'autorizzazione preventiva al Responsabile del trattamento.
- Gli strumenti di autenticazione (ad esempio, le *password*) che consentono l'accesso alle applicazioni devono essere mantenute riservate. Essi non vanno mai condivisi con altri utenti (anche se Incaricati del trattamento).
- Le *password* devono essere sostituite, a cura del singolo Incaricato, al primo utilizzo e successivamente almeno ogni sei mesi.
- Le *password* devono essere composte da almeno otto caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito. Le *password* non devono contenere riferimenti agevolmente riconducibili all'Incaricato (es. nomi propri e di familiari).

**2.2 Protezione del PC o PDL dei dati**

- Tutti i PC devono essere dotati di password.
- Tutti i PC devono essere dotati di software antivirus aggiornato costantemente.
- Sui PC devono essere installati esclusivamente software necessari all'attività lavorativa, dotati di licenza e forniti dall'Ufficio di appartenenza. Sono vietati i software scaricati da Internet o acquisiti autonomamente.
- Per evitare accessi illeciti, deve essere sempre attivato il salva schermo con password.
- Sui PC devono essere installati, appena vengono resi disponibili (e comunque almeno annualmente), tutti gli aggiornamenti software necessari a prevenirne vulnerabilità e correggerne i difetti.
- Deve essere effettuato, con cadenza almeno annuale un salvataggio di *back-up* di eventuali dati personali presenti unicamente sul PC personale (cioè non accessibili tramite i sistemi informatici ministeriali). I supporti di memoria utilizzati per il *back-up* devono essere trattati secondo le regole definite al punto "Trattamento senza l'ausilio di strumenti elettronici".

**2.3 Cancellazione dei dati dai PC**

- I dati personali conservati sui PC devono essere cancellati in modo sicuro (es. formattando i dischi) prima di destinare i PC ad usi diversi.

**2.4 Custodia**

e-mail: [usp.vr@istruzione.it](mailto:usp.vr@istruzione.it) C.F. 80011240233 - Pec: [uspvpr@postacert.istruzione.it](mailto:uspvpr@postacert.istruzione.it) - Tel. 0458086511



Ministero dell'Istruzione, dell'Università e della Ricerca  
Ufficio Scolastico Regionale per il Veneto  
**UFFICIO VII - AMBITO TERRITORIALE DI VERONA**

Viale Caduti del Lavoro, 3 - 37124 Verona

- I dati personali archiviati su supporti di tipo magnetico e/o ottico devono essere protetti con le stesse misure di sicurezza previste per i supporti cartacei.
- **2.5 Ulteriori istruzioni in caso di trattamento di dati sensibili e/o giudiziari**
- Le *password* di accesso alle procedure informatiche che trattano dati sensibili e/o giudiziari devono essere sostituite, da parte del singolo incaricato, almeno ogni tre mesi.
- L'installazione degli aggiornamenti software necessari a prevenire vulnerabilità e correggerne i difetti dei programmi per elaboratori deve essere effettuato almeno semestralmente.

### 3. ISTRUZIONI DI CARATTERE GENERALE

#### 3.1 Come scegliere e usare la password

- Usare almeno 8 caratteri, o nel caso in cui lo strumento elettronico non lo permetta, usare un numero di caratteri pari al massimo consentito.
- Non utilizzare date di nascita, nomi o cognomi propri o di parenti.
- Non sceglierla uguale al numero di telefono o alla *user-id*.
- Custodirla sempre in un luogo sicuro e non accessibile a terzi.
- Non divulgarla a terzi.
- Non condividerla con altri utenti.

#### 3.2 Come comportarsi in presenza di ospiti o di personale di servizio

- Fare attendere gli ospiti in luoghi in cui non siano presenti informazioni riservate o dati personali.
- Se è necessario allontanarsi dalla scrivania in presenza di ospiti, riporre i documenti e attivare il salva schermo del PC.
- Non rivelare o fare digitare le *password* dal personale di assistenza tecnica.
- Non rivelare le *password* al telefono né inviarla via fax in quanto nessuno è autorizzato a chiederle.
- Segnalare qualsiasi anomalia o stranezza al Responsabile.

#### 3.3 Come gestire la posta elettronica

- È sempre vietata la diffusione di dati sensibili o giudiziari.
- Non aprire messaggi con allegati di cui non si conoscono l'origine, in quanto possono contenere virus in grado di cancellare i dati sul PC.

#### 3.4 Come usare correttamente Internet

- È sempre vietata la diffusione di dati sensibili o giudiziari.
- Evitare di scaricare dalla rete file e software di uso non direttamente riferibile all'attività di lavoro, in quanto questo può essere pericoloso per i dati e la rete del MIUR. I software necessari all'attività lavorativa vanno richiesti ai consegnatari economici dei rispettivi Uffici.

### 4. SANZIONI PER INOSSERVANZA DELLE NORME

Le presenti istruzioni sono impartite ai sensi delle normative vigenti in materia di privacy; l'inosservanza delle presenti istruzioni da parte dell'Incaricato può comportare sanzioni anche di natura penale a suo carico ai sensi delle disposizioni di cui alla parte III, titolo III, capi I e II del D.Lgs. N. 196/2003 (artt. da 161 a 172 del D. Lgs. 196/2003).

Il Responsabile del trattamento dei dati  
Direttore Generale Daniela Beltrame