**OGGETTO: Tutela dei dati personali. La nuova disciplina sulla protezione delle persone fisiche con riguardo al trattamento dei dati personali prevista dal Regolamento UE 2016/679 – Designazione delle persone Incaricate al Trattamento dei Dati Personali e Istruzioni per il trattamento dei dati.**

In qualità di Titolare / Responsabile del Trattamento dei dati personali, conformemente a quanto stabilito dal Regolamento UE 679/2016 e Normativa Italiana, si incarica la S.V. come designato del trattamento dei dati personali gestiti al fine di adempiere alle attività operative del proprio ufficio e al perseguimento delle finalità istituzionali dell’ASP VITTORIO EMANUELE II di Fabriano “……… *le persone autorizzate al trattamento dei dati personali sotto l’autorità del titolare o del responsabile art. 4, c. 10 GDPR*”.

“*Il titolare o il responsabile del trattamento possono prevedere, sotto la propria responsabilità e nell’ambito del proprio assetto organizzativo, che specifici compiti e funzioni connessi al trattamento di dati personali siano attribuiti a persone fisiche, espressamente designate, che operano sotto la loro autorità” (art. 2-quaterdecies c.1, d.lgs. 101/2018*

**Nome:**

**Cognome:**

**Cod. Fis. / Par. IVA:**

**Mansione:**

**Note:**

Per opportuna informazione si allegano le seguenti istruzioni.

§§§§§§§

La S.V. dovrà attenersi ai criteri previsti dalla normativa vigente sulla tutela dei dati personali e sulle misure di sicurezza relative, anche con riferimento alle norme ed alle modalità tecniche ed organizzative adottate dal titolare del trattamento.

Al riguardo, la S.V. si impegna ad effettuare il trattamento dei dati di competenza ed a garantire la riservatezza osservando le istruzioni riportate nelle Istruzioni per il trattamento dei dati allegate alla presente che vengono consegnate in copia ed ogni altra indicazione che potrà essere fornita dal Titolare del trattamento.

## ISTRUZIONI AGLI INCARICATI DEL TRATTAMENTO DEI DATI PERSONALI COMUNI, SENSIBILI E/O GIUDIZIARI

## **(da integrare/modificare in base ad assessment)**

In ottemperanza alle vigenti disposizioni in materia di protezione dei dati personali (D. LGS 196/03 e Regolamento europeo GDPR n.678/2016) ed in relazione alle attività svolte ed ai compiti affidati, l’“Incaricato”, dovrà effettuare i trattamenti di dati personali di competenza attenendosi scrupolosamente alle seguenti istruzioni e ad ogni ulteriore indicazione, anche verbale, che potrà essere fornita dal “Titolare del trattamento” come sopra identificato.

L’incaricato del trattamento dei dati, deve rispettare il principio di pertinenza e non eccedenza rispetto alle finalità del medesimo: è consentito l’accesso solo a quei dati personali la cui conoscenza sia strettamente indispensabile per adempiere i compiti affidati. I dati devono essere esatti, aggiornati e trattati in modo lecito e secondo correttezza (art.6 GDPR 679/2016).

I dati personali devono essere trattati: a) in osservanza dei criteri di minimizzazione e riservatezza; b) in modo lecito e secondo correttezza; c) per un periodo di tempo non superiore a quello necessario agli scopi per i quali sono stati raccolti o successivamente trattati; d) nel pieno rispetto delle misure 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. Le misure tecniche organizzative individuate dal titolare del trattamento sono obbligatorie e sono distinte in funzione delle seguenti modalità di trattamento dei dati:

* senza l’ausilio di strumenti elettronici (es. dati in archivi cartacei o su supporto magnetico/ottico);
* con ausilio di strumenti elettronici (PC ed elaboratori).

## art.1 OBBLIGHI DELL’INCARICATO

L’incaricato, in particolare, nello svolgimento del trattamento, è tenuto a

* Accertare che l’informativa, completa in tutte le sue parti, venga comunicata agli interessati, *“Informazioni da fornire qualora i dati personali siano raccolti presso l’interessato art 13 del GDPR;*
* Consentire l’esercizio dei diritti e delle facoltà previste *dal Regolamento UE dall’art.15 all’art.21*, informare l’interessato dell’esistenza del trattamento dei dati che lo riguardano, delle finalità e le modalità del trattamento ed ogni altra attività connessa allo stesso;
* Provvedere previa espressa richiesta scritta dell’interessato, all’aggiornamento dei dati nonché alla loro rettifica, integrazione, cancellazione, trasformazione in forma anonima o al blocco qualora trattati in violazione della legge;
* Collaborare con gli altri incaricati del medesimo trattamento, esclusivamente per i fini dello stesso e nel rispetto delle indicazioni fornite;
* Non trasmettere a soggetti terzi, informazioni sui dati personali trattati. La comunicazione è ammessa soltanto se funzionale allo svolgimento dei compiti affidati, previa autorizzazione del Responsabile del trattamento;
* Accertarsi dell’identità del diretto interessato, prima di fornire informazioni circa i dati personali o il trattamento effettuato;
* Riporre in archivio al termine del periodo di trattamento, i supporti o i documenti, ancorché non definitivi, contenenti i dati personali;
* Conservare i dati trattati per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono raccolti e successivamente trattati.

## ART. 2 TRATTAMENTI SENZA L’AUSILIO DI STRUMENTI ELETTRONICI

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. Le misure di sicurezza applicate alle copie o alle riproduzioni dei documenti contenenti dati personali devono essere identiche a quelle applicate agli originali.

* **CUSTODIA** · I documenti contenenti dati personali, devono essere custoditi in modo da non essere accessibili a persone non incaricate del trattamento (es. armadi o cassetti 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.
* **COMUNICAZIONE** · L’utilizzo dei dati personali deve avvenire in base al principio del “need to know” 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 della scuola e comunque a soggetti terzi se non previa autorizzazione
* **DISTRUZIONE** · Qualora sia necessario distruggere i documenti contenti 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. · I supporti magnetici od ottici contenenti dati personali devono essere cancellati prima di essere riutilizzati. Se ciò non è possibile, essi devono essere distrutti.
* Ulteriori istruzioni in caso di trattamento di dati sensibili e/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 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 cassetti chiusi 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.

## art.3 TRATTAMENTI CON STRUMENTI ELETTRONICI

* 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) o in una caratteristica biometrica. 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 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 di familiari) e devono essere scelte nel rispetto della normativa di Ateneo sulla costruzione ed utilizzo delle password (vedi successivo punto 3.).

* Protezione del PC e dei dati.

Tutti i PC devono essere dotati di password rispondenti alle normative di Ateneo e, ove possibile, va impostata anche la password di BIOS. · Le password di accesso ai PC contenenti dati personali, nonché le eventuali password per l’accesso ai singoli file contenenti tali dati devono essere consegnate in busta chiusa al Custode delle parole chiave. · Tutti i PC devono essere dotati di software antivirus aggiornato costantemente e con la funzione “Monitor” attiva. · Sui PC devono essere installati esclusivamente software necessari all’attività lavorativa, dotati di licenza e forniti dalle strutture 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 settimanale un salvataggio di back-up di eventuali dati personali presenti unicamente sul PC personale (cioè non accessibili tramite i sistemi informatici universitari). 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”.

* 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.

* 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.

## art.4 ISTRUZIONI DI CARATTERE GENERALE

Come scegliere e usare la password (Normativa sulla costruzione ed utilizzo delle 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. · Usare lettere, numeri e almeno un carattere tra ; $ ! @ - > < - Non utilizzare date di nascita, nomi o cognomi propri o di parenti · Non sceglierla uguale alla matricola o alla user-id · Custodirla sempre in un luogo sicuro e non accessibile a terzi · Non divulgarla a terzi · Non condividerla con altri utenti.

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 salvaschermo del PC. · Non rivelare o fare digitare le password dal personale di assistenza tecnica. · Non rivelare le password al telefono né inviarla via fax - nessuno è autorizzato a chiederle. · Segnalare qualsiasi anomalia o stranezza al Responsabile.

Come gestire la posta elettronica:

Non aprire messaggi con allegati di cui non si conoscono l’origine, possono contenere virus in grado di cancellare i dati sul PC. · Evitare di aprire filmati e presentazioni non attinenti l’attività lavorativa per evitare situazioni di pericolo per i dati contenuti sul vostro PC.

Come usare correttamente Internet:

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 d’azienda. I software necessari all’attività lavorativa vanno richiesti alle competenti strutture universitarie. · Usare Internet solo per lavoro, i siti web spesso nascondono insidie per i visitatori meno esperti. · Non leggere le caselle personali esterne via webmail in quanto alcuni provider esterni non proteggono dai virus.

## ART. 5 IN CASO DI PRESENZA DI OSPITI/UTENTI O LORO PARENTI.

1. Fare attendere in luoghi in cui non sono presenti informazioni riservate o dati personali;
2. Evitare di allontanarsi dalla scrivania in presenza di ospiti, riporre in armadi provvisti di serratura i documenti, attivare il salvaschermo del PC;
3. Non rivelare o far digitare la password ai colleghi;
4. Non rivelare le password al telefono né inviarle via fax e nessuno è autorizzato a chiederle;
5. Segnalare qualsiasi anomalia o stranezza al Responsabile del trattamento.

## ART. 6 MODALITA’ DI TRATTAMENTO DATI PERSONALI PARTCIOLARI (sensibili) E GIUDIZIARI

Fermo restando l’applicazione delle disposizioni vigenti in materia di trattamento dei dati personali particolari e giudiziari “Trattamento di categorie particolari di dati personali art. 9 GDPR 679/2016” e delle istruzioni impartite dal Responsabile del trattamento, si riportano alcune specifiche misure da applicarsi in caso di trattamento dei predetti dati.

**1.** Non fornire dati o informazioni di carattere “sensibile” per telefono, qualora non si abbia certezza assoluta sull’identità del destinatario;

Evitare di inviare, per fax documenti in chiaro contenenti dati “personali” per come indicato nel RGDP all’art. 9 che comprendono:

- dati sensibili (che rivelino “l’origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l’appartenenza sindacale”),

- dati genetici e dati biometrici (intesi ad identificare in modo univoco una persona fisica),

- dati sanitari (dati relativi alla salute o alla vita sessuale o all’ orientamento sessuale della persona etc..) si suggerisce, in tal caso, di inviare la documentazione, senza alcun esplicito riferimento all’interessato;

**2.** I documenti elettronici ancorché non definitivi, i supporti o documenti cartacei, recanti dati personali, particolari (sensibili) o giudiziari, devono essere conservati dagli incaricati, per la durata del trattamento, in armadi muniti di serratura al fine di escludere l’acquisizione da parte di persone non autorizzate al trattamento e non devono essere lasciati incustoditi in assenza dell’incaricato;

**3.** Concluso il trattamento dei dati personali, i documenti elettronici, cartacei e i supporti saranno riposti in archivi ad accesso controllato al fine di escludere l’accesso a persone non incaricate al trattamento;

**4.** Al fine di salvaguardare la riservatezza dei dati personali, si ritiene opportuno adottare misure organizzative riguardo ai flussi di documenti cartacei tra i diversi uffici (es. trasmissione dei documenti in buste chiuse);

**5.** Qualora fosse necessario distruggere i documenti contenenti dati personali, utilizzare gli appositi apparecchi “distruggi documenti”. In assenza di tali strumenti, i documenti devono essere sminuzzati in modo da non essere più ricomponibili.

## art.7 AVVISO IN CASO DI INCIDENTE.

Informare immediatamente il Titolare del trattamento nel caso di qualsiasi malfunzionamento dei sistemi informativi, minaccia o incidente alla sicurezza dei dati.

## art.8 SANZIONI PER INOSSERVANZA DELLE NORME

Le presenti istruzioni sono impartite ai sensi delle normative vigenti in materia di privacy, l’inosservanza delle quali da parte dell’Incaricato può comportare sanzioni civili e penali a suo carico.

La presente lettera deve essere sottoscritta solamente per ricevuta e costituisce un atto di documentata preposizione allo svolgimento di trattamenti, necessario per consentire a ciascun dipendente o collaboratore dell’ASP di svolgere le operazioni di trattamento, necessarie all’esercizio delle mansioni e dei compiti istituzionali.

Per ricevuta di copia delle presenti istruzioni

NOME COGNOME FIRMA

………………………………………….…………………… ……....……………………………………