Università Ca' Foscari Venezia
Dorsoduro 3246, 30123 Venezia
P.IVA 00816350276 - CF 80007720271
www.unive.it

Decreto della Rettrice 2021

Oggetto: Designazione ad Autorizzato al trattamento ai sensi dell'art. 16 del Regolamento in materia di protezione dei dati personali dell'Università Ca' Foscari Venezia, dell'art. 29 del Regolamento (UE) 2016/679 e dell'art. 2-*quaterdecies* del D.Lgs. n. 196/2003.

LA RETTRICE

VISTO il Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE ("***General Data Protection Regulation***" - "**GDPR**");

VISTO lo Statuto di Ateneo;

CONSIDERATO il processo di adeguamento al GDPR che ha riguardato l'intera organizzazione interna e ha, pertanto, comportato il coinvolgimento di competenze multidisciplinari;

CONSIDERATO che, in ossequio al principio di responsabilizzazione (c.d. *accountability*) di cui all'art. 24 del GDPR, l'Università Ca' Foscari Venezia ("**Università**" o "**Titolare**") ha definito una struttura organizzativa privacy, meglio descritta all'interno del "*Regolamento in materia di protezione dei dati personali*" adottato dall'Università ("**Regolamento interno**");

PRESO ATTO che l'Università, in qualità di Titolare del trattamento, ha inoltre provveduto alla designazione del *Data Protection Officer* o Responsabile della Protezione dei Dati ("**DPO**") ai sensi dell'art. 37 del GDPR;

VISTO l'art. 15 del Regolamento interno, che attribuisce specifici compiti a coloro che ricoprono ruoli di impulso e coordinamento all'interno delle Aree dell'Amministrazione Centrale, dei Dipartimenti, delle Scuole, dei Centri e del Sistema Bibliotecario dell'Università ("**Struttura**" o "**Strutture**");

CONSIDERATO che il Regolamento interno prevede la designazione delle seguenti figure: Referente di Struttura, Referente Interno e Autorizzato al trattamento;

PRESO ATTO che i Referenti di Struttura sono individuati nella persona del Direttore Generale, dei Dirigenti delle Aree dell'Amministrazione Centrale, del Sistema Bibliotecario e del Centro Linguistico di Ateneo, dei Direttori dei Dipartimenti e dei Responsabili dei Centri e delle Scuole dell'Università con funzioni di rappresentanza e ricoprono un ruolo di indirizzo, coordinamento, controllo, nonché di programmazione della formazione del personale interno alla propria Struttura, in collaborazione con il DPO;

PRESO ATTO che i Referenti Interni sono individuati nella persona dei Direttori degli Uffici, dei Segretari dei Dipartimenti, delle Scuole e dei Centri, dei Direttori di Biblioteca e dei Responsabili Scientifici di Attività di Ricerca che comporti un trattamento di dati personali (a titolo esemplificativo e non esaustivo, coordinatori di attività di ricerca, referenti scientifici di un progetto di ricerca finanziato, *tutor* di assegnisti di ricerca,

relatori di tesi di laurea o di dottorato, ecc.), attribuendo loro un ruolo operativo, finalizzato all'esecuzione degli interventi programmatici definiti dal Referente di Struttura ovvero al corretto trattamento dei dati personali all'interno dell'Attività di Ricerca, oltreché compiti di collaborazione con il DPO e doveri di supervisione e formazione nei confronti dei soggetti che operano all'interno della Struttura di appartenenza ovvero dei Ricercatori che collaborano all'Attività di Ricerca;

PRESO ATTO che tutti i soggetti che trattano dati personali per conto dell'Università (in particolare il personale tecnico-amministrativo – compresi i tecnologi di cui all'art. 24-bis della L. n. 240/2010 –, i collaboratori ed esperti linguistici (CEL), i professori universitari, i ricercatori anche a tempo determinato, i docenti a contratto, i *visiting professor* e i *visiting scholar*, i dottorandi, gli assegnisti, i borsisti, i consulenti e collaboratori e gli eventuali altri soggetti che intrattengono rapporti di lavoro o collaborazione con l'Università, compresi gli studenti nello svolgimento delle attività di supporto ai servizi universitari, e gli stagisti nonché i volontari del servizio civile assegnati all'Università) devono essere designati da quest'ultima Autorizzati al trattamento ai sensi degli artt. 29 e 32, c. 4, del GDPR e dell'art. 2-*quaterdecies* del D.Lgs. n. 196/2003, come previsto dall'art. 16 del Regolamento interno ("**Autorizzati**");

CONSIDERATO che gli Autorizzati, pur operando sotto la diretta autorità del Titolare, sono soggetti all'attività di coordinamento e controllo del Referente di Struttura e Referente Interno di riferimento e devono rispettare le disposizioni del GDPR, del D.Lgs. n. 196/2003 e dei Provvedimenti del Garante per la Protezione dei Dati Personali ("**Normativa privacy**"), del Regolamento interno e delle istruzioni e linee guida redatte in collaborazione con il DPO ("**Regole operative**");

PRESO ATTO che la struttura proponente ha attestato la conformità del provvedimento alla legislazione vigente e ai regolamenti di Ateneo.

DECRETA

Art. 1 Il personale tecnico-amministrativo – compresi i tecnologi di cui all'art. 24-bis della L. n. 240/2010 –, i collaboratori ed esperti linguistici (CEL), i professori universitari, i ricercatori anche a tempo determinato, i docenti a contratto, i *visiting professor* e i *visiting scholar*, i dottorandi, gli assegnisti, i borsisti, i consulenti e collaboratori e gli eventuali altri soggetti che intrattengono rapporti di lavoro o collaborazione o con l'Università, compresi gli studenti nello svolgimento delle attività di supporto ai servizi universitari, e gli stagisti nonché i volontari del servizio civile assegnati all'Università sono designati Autorizzati al trattamento e sono loro attribuiti i compiti di seguito indicati:

a. trattare i dati personali con la massima diligenza in considerazione all'attività eseguita e al rapporto intrattenuto;
b. accedere ai soli dati personali il cui trattamento è strettamente necessario per adempiere alle proprie mansioni e trattare i predetti dati esclusivamente per il raggiungimento delle finalità e nel rispetto delle esigenze operative dell'Università,

attenendosi scrupolosamente alle disposizioni della Normativa privacy e del Regolamento interno, così come richiamate e declinate nelle Regole operative;

c. astenersi dall'utilizzare i dati personali per scopi diversi da quelli inerenti alle proprie mansioni, e ciò anche successivamente alla cessazione, per qualsiasi ragione o titolo, del rapporto con l'Università;
d. attenersi ai doveri di riservatezza e di fedeltà, laddove previsti, astenendosi dal comunicare i dati personali a soggetti non autorizzati, anche dopo la cessazione del rapporto con l'Università e conseguentemente della presente nomina;
e. partecipare ai corsi di formazione sulla Normativa privacy individuati come obbligatori dal Titolare entro il termine previsto da quest'ultimo, nonché a tutti gli ulteriori eventi programmati dal Referente di Struttura e/o dal Referente Interno;
f. rispettare le misure di sicurezza tecniche e organizzative individuate dall'Università nel Regolamento interno e nelle Regole operative, riassunte nell'allegato Vademecum "*Nozioni generali in materia di protezione dei dati personali*" ("**Vademecum**"); nel dettaglio, l'Autorizzato dovrà:
    i) adottare tutte le necessarie cautele per assicurare la segretezza della componente riservata della propria credenziale di autenticazione (password) nel rispetto delle prescrizioni contenute nell'art. 2 dell'Allegato B del Regolamento interno;
    ii) custodire i dati personali oggetto di trattamento sotto la propria responsabilità diretta, conservandoli unicamente all'interno degli archivi e delle cartelle messi a disposizione dall'Università, al fine di impedire che possano essere conosciuti da soggetti non autorizzati anche facenti parte dell'Università, come previsto dall'art. 2 dell'Allegato C al Regolamento interno;
    iii) utilizzare gli strumenti di lavoro messi a disposizione dall'Università unicamente per lo svolgimento della mansione attribuita, nel rispetto delle previsioni dell'art. 3 dell'Allegato C al Regolamento interno, evitando di scaricare e/o installare software senza l'autorizzazione dell'Area Servizi Informatici e Telecomunicazioni ("**ASIT**");
    iv) astenersi dall'installare strumenti hardware e/o software atti a intercettare e a modificare le comunicazioni informatiche oppure ad aggirare o a neutralizzare i sistemi di protezione installati dall'Università nel rispetto delle previsioni dell'art. 3 dell'Allegato C al Regolamento interno;
    v) astenersi dal trasmettere, scaricare, stampare o diffondere in qualunque altro modo contenuti di carattere indecente, osceno, razzista, sessualmente esplicito, illegale, immorale o discriminatorio nel rispetto delle previsioni dell'art. 3 dell'Allegato C al Regolamento interno;
    vi) mantenere aggiornato il software antivirus installato dall'Università sui *device* che gli sono stati assegnati per lo svolgimento della propria attività nel rispetto delle previsioni dell'art. 3 dell'Allegato C al Regolamento interno;

vii) custodire i *device* utilizzati per lo svolgimento della propria attività con la massima diligenza; durante l'utilizzo del *device*, in caso di allontanamento anche temporaneo, bloccare le funzionalità del sistema, nonché, al termine dell'attività, effettuare il *log-off* dai sistemi nel rispetto delle previsioni dell'art. 3 dell'Allegato C al Regolamento interno;

viii) conservare gli atti e i documenti in formato cartaceo in modo da evitare distruzioni o accessi da parte di terzi non autorizzati;

ix) custodire in armadi chiusi a chiave i documenti cartacei contenenti dati particolari e giudiziari;

x) conservare in luoghi protetti i supporti di memoria rimovibili contenenti dati personali nel rispetto delle previsioni dell'art. 3 dell'Allegato C al Regolamento interno;

xi) trasmettere i dati personali all'interno dell'Università esclusivamente ai soggetti che hanno necessità di accedervi per lo svolgimento della propria attività, come previsto dall'art. 26 del Regolamento interno;

xii) comunicare i dati personali a soggetti esterni all'Università solamente in adempimento di un obbligo di legge e, ove necessario, a fronte di richiesta esplicita, scritta e motivata ai sensi dell'art. 27 del Regolamento interno;

xiii) utilizzare appropriate tecniche di cifratura individuate dall'Università in caso di memorizzazione e/o trasmissione di categorie particolari di dati personali, nel rispetto delle procedure disponibili alla pagina https://www.unive.it/criptarearchivi;

xiv) diffondere i dati personali solo ove previsto da una norma di legge applicabile, verificando le specifiche modalità individuate all'interno del Regolamento interno in relazione alla particolare fattispecie;

xv) cancellare, secondo le indicazioni contenute all'art. 3 dell'Allegato C al Regolamento interno e con l'eventuale supporto di ASIT, i dati contenuti nei supporti rimovibili, quando non più necessari;

xvi) utilizzare la posta elettronica e la rete internet dell'Università unicamente per finalità istituzionali, rispettando gli obblighi previsti dall'art. 4 dell'Allegato D del Regolamento interno;

g. informare tempestivamente il Referente di Struttura, il Referente Interno o, alternativamente, il DPO, di ogni problematica relativa al trattamento dei dati personali;

h. informare di eventuali casi di violazione della sicurezza, entro 6 ore dall'avvenuta conoscenza, l'Ufficio Supporto Utenti di ASIT (tramite e-mail e telefonate), nel rispetto della "*Policy per la gestione dei Data Breach*" adottata dall'Università, nonché il Referente di Struttura, il Referente Interno e il DPO; in particolare, si ha violazione di sicurezza in caso di eventi che comportino accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso non autorizzato ai dati personali trasmessi, conservati;

Università Ca' Foscari Venezia
Dorsoduro 3246, 30123 Venezia
P.IVA 00816350276 - CF 80007720271
www.unive.it

i. collaborare in occasione delle verifiche, anche secondo quanto illustrato nell'Allegato E del Regolamento interno, che verranno svolte dall'Università anche mediante il Referente Interno, il DPO o eventuali altri soggetti delegati, al fine di assicurare la rigorosa applicazione della Normativa privacy, del Regolamento interno e delle Regole operative, nonché il corretto rispetto delle finalità e modalità del trattamento dei dati personali determinate dal Titolare.

Art. 2 I dati personali, le finalità, le attività di trattamento che possono essere svolte dai singoli Autorizzati, nonché le Regole operative che devono essere rispettate sono indicati nelle schede del Registro delle attività di trattamento relative alla/e mansione/i degli stessi. Le specifiche schede e le Regole operative per il corretto adempimento dei compiti elencati all'art. 1 del presente Decreto saranno fornite agli Autorizzati dal Referente Interno di riferimento. È fatto comunque obbligo all'Autorizzato di richiedere tali informazioni al proprio Referente Interno.

Art. 3 Il Vademecum è da considerarsi parte integrante del presente Decreto. Resta fermo comunque l'obbligo per gli Autorizzati di prendere visione e di rispettare il contenuto integrale del Regolamento interno e delle Regole operative di propria competenza.

Art. 4 La violazione degli obblighi attribuiti con la presente nomina può esporre a profili di responsabilità disciplinare, con conseguente possibilità di assoggettamento, a seconda della gravità della singola mancanza, a una delle sanzioni disciplinari previste dal CCNL di riferimento e dalla legge.

Art. 5 L'assunzione della qualifica di Autorizzato non comporta alcun riconoscimento economico in quanto normativamente necessaria per lo svolgimento delle attività di trattamento dei dati personali svolte per conto dell'Università.

Art. 6 La designazione di cui ai precedenti articoli decorre dal 1° marzo 2022 e si intende priva di scadenza salvo eventuale aggiornamento da effettuarsi con medesimo provvedimento.

La Rettrice
Prof.ssa Tiziana Lippiello

Allegato: Vademecum "*Nozioni generali in materia di protezione dei dati personali*"

VISTO IL RESPONSABILE DEL PROCEDIMENTO AMMINISTRATIVO
Dott.ssa Monica Gussoni

VISTO IL DIRETTORE GENERALE
Dott. Gabriele Rizzetto

Università Ca' Foscari Venezia
Dorsoduro 3246, 30123 Venezia
P.IVA 00816350276 - CF 80007720271
www.unive.it

Vademecum "*Nozioni generali in materia di protezione dei dati personali*"

DATI PERSONALI	
Cos'è un dato personale?	Qualsiasi informazione che permette di identificare una persona fisica direttamente (es. attraverso nome e cognome) o indirettamente, tramite qualsiasi altra informazione relativa ad esempio alle abitudini, alle relazioni personali, allo stato di salute, alla situazione economica o lavorativa (es. il Dirigente dell'Area Risorse Umane dell'Università), ivi compreso un numero d'identificazione personale (come il codice fiscale, il numero di matricola e l'indirizzo IP, l'immagine, la voce, la grafia, ecc).
Dati personali comuni	Informazioni riferite a una persona fisica quali, per esempio, i dati anagrafici (nome, cognome, data di nascita, codice fiscale e indirizzo di residenza), la partita IVA, il numero di telefono e l'indirizzo e-mail.
CATEGORIE DI DATI PERSONALI CHE, PER LA LORO PARTICOLARE NATURA, NECESSITANO DI TUTELE RAFFORZATE	
Dati particolari	Si tratta dei cosiddetti *"dati sensibili"*, cioè quelli che rivelano l'origine razziale od etnica, le convinzioni religiose, filosofiche, le opinioni politiche, l'appartenenza sindacale, relativi alla salute o alla vita sessuale ("dati sanitari"); in questa categoria rientrano anche i dati genetici (relativi cioè alle caratteristiche genetiche ereditarie), i dati biometrici (relativi alle caratteristiche fisiche, fisiologiche o comportamentali di un individuo rilevate attraverso tecnologie innovative, come la scansione della retina o il riconoscimento facciale) e quelli relativi all'orientamento sessuale.
Dati giudiziari	Informazioni relative a provvedimenti giudiziari soggetti ad iscrizione nel casellario giudiziale (ad esempio, i provvedimenti penali di condanna definitivi, la liberazione condizionale, il divieto od obbligo di soggiorno), condanne penali, reati, alla qualità di imputato o di indagato.
I SOGGETTI PRIVACY	
Titolare	La persona fisica, l'autorità pubblica, l'impresa, l'ente pubblico o privato, l'associazione, ecc., che adotta le decisioni sugli scopi e sulle modalità del trattamento. *Per l'Ateneo, il Titolare è l'Università stessa in persona della Rettrice.*
Responsabile	La persona fisica o giuridica alla quale il Titolare affida la gestione di un qualsiasi servizio avente ad oggetto dati personali. *Per l'Ateneo, i Responsabili sono tutti i soggetti che forniscono all'Università servizi che comportano il trattamento di dati personali per conto della stessa. Con tali soggetti deve essere sottoscritto apposito contratto (atto di nomina a responsabile del trattamento).*
Interessato	La persona fisica alla quale si riferiscono i dati personali. Quindi, se un trattamento riguarda, ad esempio, l'indirizzo e il codice fiscale di Mario Rossi, questa persona è l'Interessato. *Per l'Ateneo, gli interessati sono, per esempio, gli studenti, il personale PTA e docente, i partecipanti a progetti di ricerca, ecc.*
IL TRATTAMENTO	
Che cosa si deve intendere per "trattamento"?	Qualsiasi attività, operazione o insieme di operazioni aventi ad oggetto dati personali effettuate con o senza l'ausilio di strumenti elettronici (supporti cartacei) come la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca dati.

Raccolta: *è la prima operazione di trattamento e*	***Registrazione:*** *l'annotazione cartacea o*	***Organizzazione/Strutturazione:*** *la classificazione e catalogazione dei dati*

consiste nell'attività di acquisizione del dato.	*memorizzazione dei dati su un qualsiasi supporto.*	*secondo un metodo prescelto e condiviso.*
Visualizzazione: *il leggere/prendere visione dei dati. Es. accesso a documenti, file o applicativi e piattaforme informatiche contenenti dati personali.*	***Modifica:*** *la parziale trasformazione o variazione dei dati trattati. Es. correzione, aggiornamento, alterazione di dati.*	***Conservazione:*** *la custodia in archivi cartacei o memorizzazione di informazioni digitali su un qualsiasi supporto informatico. Es. archivi, magazzini di fascicoli, hard disk, pendrive, back-up, copie di sicurezza.*
Distruzione: *l'attività di eliminazione definitiva dei dati trattati mediante strumenti cartacei utilizzando strumenti (per es. trita documenti) o servizi specializzati.*	***Cancellazione:*** *l'eliminazione di dati raccolti mediante strumenti elettronici. Es. cancellazione, in modo irreversibile, di file, database o parte di essi.*	***Comunicazione:*** *il dare conoscenza di dati personali ad uno o più soggetti determinati diversi dall'Interessato, dal Responsabile del trattamento e dagli autorizzati, anche mediante la loro messa a disposizione o consultazione.* *Es. invio dei dati dei dipendenti all'INPS o invio di e-mail contenenti dati personali a consulenti o avvocati.*
Diffusione: *il dare conoscenza dei dati trattati ad un numero di soggetti indefinito, in qualunque forma anche mediante la loro messa a disposizione o consultazione Es. pubblicazione delle graduatorie sul sito web.*		

QUALI PRINCIPI GENERALI DEVONO "GUIDARE" IL MIO TRATTAMENTO?	
Need to know	I dati devono essere conosciuti solo da chi ha l'effettiva necessità di accedervi per svolgere i propri compiti (es. un dipendente dell'area Risorse Umane, potrà aver accesso ai dati dei dipendenti e collaboratori necessari per lo svolgimento della propria attività, ma non dovrà aver accesso ai dati degli studenti dell'Ateneo, salvo che ciò non sia necessario, per esempio, nell'ambito di un procedimento disciplinare).
Integrità, Riservatezza e Disponibilità	I dati devono essere trattati in modo da garantire un livello di sicurezza adeguato al rischio.
Liceità del trattamento	I dati devono essere trattati sulla base di una idonea base giuridica (l'Università può trattare i dati personali solo per finalità istituzionali sulla base di un obbligo di legge).
Correttezza del trattamento	Rispettare tutte le norme che regolano quel trattamento specifico (es. nel caso di installazione di impianti di videosorveglianza rispettare le prescrizioni dello Statuto dei Lavoratori e i provvedimenti delle Autorità Privacy nazionali e Europee).
Trasparenza	Prima di raccogliere i dati, informare l'interessato con un linguaggio semplice e chiaro (ossia verificare che sia stata resa idonea informativa).
Finalità Determinate, Esplicite e Legittime	Prima dell'inizio del trattamento stabilire per quali scopi si intende raccogliere i dati e dichiararlo chiaramente agli interessati.
Principio Di Necessità	Evitare di identificare l'interessato quando il trattamento non lo richiede o non è necessario (es. in caso di questionario da compilare a fini statistici) e di raccogliere dati superflui per il raggiungimento della finalità perseguita.
Esattezza	I dati trattati devono essere esatti e costantemente aggiornati (es. dare riscontro alle richieste di rettifica dei dati avanzate dagli interessati).
Limitazione Della Conservazione	I dati devono essere conservati solo per il tempo strettamente necessario al raggiungimento della finalità per la quale sono stati raccolti salvo sussista una base giuridica per il trattamento per ulteriori finalità (es. i dati raccolti per la partecipazione ad eventi di orientamento, dovranno essere cancellati

	decorso il periodo di conservazione stabilito. Le immagini raccolte dagli impianti di videosorveglianza devono essere cancellate entro 48 ore salvo i periodi di chiusura dell'Università o ove sia stato commesso o si sospetti sia stato commesso un reato).
Trasparenza	Prima di raccogliere i dati, informare l'interessato con un linguaggio semplice e chiaro (ossia verificare che sia stata resa idonea informativa).

QUALI SONO LE REGOLE RELATIVE ALLA PASSWORD DELL' ACCOUNT UNIVE?

L'accesso all'account unive avviene tramite username e password.

La password **deve**:

- essere modificata al primo accesso e, successivamente, ogni 180 giorni;
- essere composta da almeno 10 caratteri alfanumerici e presentare almeno: un carattere numerico, un carattere maiuscolo, un carattere minuscolo e un carattere speciale all'interno di un insieme definito e indicato all'utente in fase di inserimento (es. Ahgt59!E?$).
- essere modificata immediatamente ogni qualvolta sussista il rischio che questa sia facilmente conoscibile o sia stata effettivamente conosciuta da terzi ovvero su richiesta esplicita di ASIT ove vengano rilevate compromissioni della password.

La password **non deve**:

- contenere parole o parti di parola di uso comune (es. venez123) o sequenze comuni di caratteri o numeri (es. 123456 qwerty aaaaa) e non deve essere stata utilizzata nei precedenti 12 mesi;
- contenere elementi agevolmente riconducibili all'utente o riferimenti basati su informazioni facilmente deducibili, quali il proprio nome, il nome dei famigliari, la data di nascita, il codice fiscale;
- essere divulgata a terzi né trascritta su supporti fisici (es. fogli, post-it, agende, ecc...);
- essere condivisa con altri (es. colleghi, familiari, ecc...) che operino con tale identificativo.

QUALI SONO LE REGOLE RELATIVE ALL'UTILIZZO DELLA CASELLA DI POSTA ELETTRONICA @unive?

La casella di posta @unive deve essere utilizzata esclusivamente per lo svolgimento dell'attività lavorativa. È tollerato un limitato utilizzo a fini privati, che non dovrà però in alcun modo interferire con il normale svolgimento dell'attività lavorativa.

La casella di posta elettronica è strettamente personale: le credenziali di accesso (username e password) non possono essere rivelate a terzi e l'account non può essere condiviso o ceduto ad altri.

Quando si utilizza la casella di posta elettronica @unive si **deve**:

- prestare attenzione nell'aprire gli allegati ricevuti, dato che rappresentano un mezzo molto diffuso per la trasmissione di virus e *malware*;
- mantenere i file ricevuti nella casella di posta elettronica o salvati nei server preposti e non nell'*hard disk* dei *personal computer*;
- inserire gli indirizzi dei destinatari nel campo "ccn" quando vengono inviate comunicazioni ad indirizzi plurimi e non deve essere resa conoscibile l'identità degli altri destinatari.

La casella di posta elettronica @unive **non deve** essere utilizzata per:

- inviare messaggi in forma anonima o sotto mentite spoglie;
- inviare messaggi il cui contenuto sia lesivo dell'immagine dell'Ateneo o sia di natura oltraggiosa, minacciosa, oscena, intimidatoria, diffamatoria, molesta e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica, o altrimenti illegali;
- violare la normativa sui diritti di autore, di proprietà intellettuale e/o industriale o, in generale, altri diritti tutelati dalla normativa vigente;
- inviare *spam* o comunicazioni di simile natura;
- inviare materiali, contenenti dati particolari, salvo previa criptazione secondo le istruzioni impartite dall'Ateneo.

Università Ca' Foscari Venezia
Dorsoduro 3246, 30123 Venezia
P.IVA 00816350276 - CF 80007720271
www.unive.it

QUALI SONO LE REGOLE RELATIVE ALL' UTILIZZO DELLE CARTELLE CONDIVISE E DEGLI SPAZI DI ARCHIVIAZIONE PERSONALI (ad es. Google Drive)?	
Si deve: ● utilizzare tali spazi per finalità istituzionale; ● procedere al salvataggio dei documenti di lavoro.	**Non si deve:** ● utilizzare tali spazi per salvare documenti personali, nemmeno per breve tempo. Durante le attività di controllo, questi documenti potrebbero essere rimossi.
QUALI SONO LE REGOLE RELATIVE ALL'UTILIZZO DEI *DEVICE* E DELLE POSTAZIONI DI LAVORO?	
Si deve: ● custodire qualunque tipo di dispositivo rimovibile in luogo protetto (es. armadi e cassettiere chiusi a chiave); ● crittografare i dati particolari prima di salvarli su supporti rimovibili; ● verificare il contenuto informativo dei supporti di memoria prima: (i) della loro consegna a terzi per il riutilizzo del supporto ovvero della loro eliminazione/distruzione (in questo caso il dispositivo non dovrà più contenere dati leggibili o comunque in qualsiasi modo recuperabili); (ii) della loro consegna a terzi per il trasferimento dei dati (in questo caso il dispositivo deve contenere esclusivamente i dati a cui il terzo ha diritto di accedere); ● cancellare i dati contenuti nei supporti rimovibili, quando non più necessari.	**Non si deve:** ● installare alcun tipo di software senza preventiva autorizzazione da parte di ASIT; ● installare strumenti hardware e/o software atti a intercettare e a modificare le comunicazioni informatiche oppure ad aggirare o a neutralizzare sistemi di protezione; ● sviluppare programmi informatici che interferiscano con l'attività di altri utenti o che modifichino parti dei sistemi informatici esistenti; ● trasmettere, scaricare, stampare o diffondere in qualunque altro modo contenuti di carattere indecente, osceno, razzista, sessualmente esplicito, illegale, immorale o discriminatorio; ● lasciare incustodita la propria postazione durante una sessione di lavoro, anche in caso di breve assenza senza proteggerla tramite le funzionalità di sistema (Ctrl+Alt+Canc); al termine dell'attività lavorativa le sessioni di lavoro devono essere chiuse (*log-off*).
QUALI SONO LE REGOLE RELATIVE UTILIZZO DELLA RETE INTERNET DELL'UNIVERSITA'?	
La rete internet dell'Università deve essere utilizzata per finalità istituzionali, ma è consentito l'uso sporadico od occasionale della stessa per motivi personali o non collegati alle attività lavorative.	
L'uso istituzionale della rete internet: ● è strettamente personale; ● non può essere finalizzato a scopi illeciti, quali la violazione di norme di legge e/o di regolamento.	L'uso personale della rete internet **non deve**: ● interferire con la produttività o con la prestazione professionale dell'utente o di qualsiasi altro dipendente; ● incidere negativamente sul buon funzionamento del computer; ● violare le norme oggetto del Regolamento interno.