

# ISTRUZIONI PER IL CORRETTO TRATTAMENTO DEI DATI PERSONALI

*Sono fornite di seguito le istruzioni necessarie a garantire il corretto trattamento dei dati personali in coerenza con gli obiettivi dell'Università perseguiti e nel rispetto dei principi generali in materia di protezione dei dati personali che devono essere rispettati da tutti i dipendenti o collaboratori a qualsiasi titolo in qualità di incaricati.*

*Le istruzioni potranno essere soggette ad eventuali aggiornamenti. La versione aggiornata è sempre disponibile all'indirizzo: <http://www.uniroma3.it/privacy/>.*

## Sommario

PREMESSA .....	3
Scopo del documento .....	3
Principi guida dell'azione amministrativa .....	3
Livelli adeguati di sicurezza .....	3
OBBLIGHI .....	5
Trattamento dei dati personali .....	5
Accesso ad archivi cartacei o a banche dati .....	6
Responsabilità .....	7
ISTRUZIONI OPERATIVE .....	8
Come posso sapere se è consentito compiere un determinato trattamento? .....	8
Posto che il trattamento non è indicato nelle Informative, posso comunque eseguirlo? .....	8
Cosa fare se dati personali sono stati sottratti, comunicati/diffusi a persone terze non autorizzate? .....	10
Conserva sempre il consenso rilasciato dall'interessato .....	10
Gestisci la distanza di cortesia .....	10
Non comunicare dati personali a soggetti non legittimati .....	11
Utilizza le chiavi .....	11
Cura la spedizione dei documenti .....	11
Conserva i documenti cartacei nel modo corretto .....	11
Fai attenzione a come distruggi i documenti .....	11
Non lasciare in vista documenti .....	12
Raddoppia le attenzioni se i documenti contengono dati particolarmente sensibili .....	12
Non dimenticare le stampe dei documenti .....	12
Limita l'uso di supporti di memorizzazione portatili .....	12
La password è personale .....	12
Non comunicare mai la tua password a seguito di una mail .....	13
Utilizza le password in modo corretto .....	13
Blocca sempre i dispositivi informatici quando non li utilizzi .....	13
Non farti sbirciare quando digiti le password .....	13
Custodisci le password in un luogo sicuro .....	14
Scegli bene la tua password .....	14
Per ogni account usa password differenti .....	14

Cosa non devi fare con la tua password .....	14
Presta attenzione all'utilizzo dei personal computer portatili o tablet .....	14
Non utilizzare dispositivi non autorizzati .....	15
Non installare programmi non autorizzati .....	15
Non utilizzare strumenti di comunicazione, memorizzazione e condivisione non autorizzati .....	15
Applica con cura le linee guida per la prevenzione da infezioni di virus .....	15
Diffida delle mail sospette.....	16
Non utilizzare la mail istituzionale per la registrazione a servizi personali.....	16
Fai attenzione a come distruggi i supporti di memorizzazione .....	16
Ricordati di fare sempre il backup .....	16
Dove puoi posizionare i server .....	17
<b>ISTRUZIONI OPERATIVE PER IL WEB .....</b>	<b>18</b>
Cancella fisicamente i file dal server web .....	18
Non pubblicare gli esiti degli esami .....	18
Limita le informazioni pubblicate nelle graduatorie.....	18
Non pubblicare mai documenti con le firme autografe.....	18
<b>ISTRUZIONI OPERATIVE PER LA VIDEO SORVEGLIANZA.....</b>	<b>20</b>
Posiziona correttamente il cartello.....	20
Limita la visuale di ripresa .....	20
Proteggi i monitor e i registratori .....	20
Cancella i supporti .....	20
La diffusione è vietata.....	20
<b>ISTRUZIONI OPERATIVE PER I SOCIAL NETWORK .....</b>	<b>21</b>
L'identificazione non è sicura .....	21
Non pubblicare alcun dato personale.....	21
Disattiva la Geo-localizzazione .....	21
<b>ISTRUZIONI OPERATIVE PER LA PREVENZIONE DEI VIRUS .....</b>	<b>22</b>
<b>INFORMAZIONI SUGLI STRUMENTI DI COLLABORAZIONE DISPONIBILI .....</b>	<b>23</b>
Filesender .....	23
OneDrive .....	24
Outlook.....	24
Sharepoint .....	24

## PREMESSA

### Scopo del documento

Nell’ottica di un efficace tutela delle informazioni e dei dati personali gestiti dall’Università degli Studi Roma Tre, il presente documento ha lo scopo di fornire le prescrizioni e le istruzioni circa il complesso delle misure organizzative, logistiche, tecniche, ed informatiche da adottare in tutte le strutture dell’Università, affinché il livello di protezione dei dati personali oggetto di trattamento sia conforme, nel quadro dei più generali obblighi di sicurezza, a quanto previsto dal Regolamento UE 2016/679 (*General Data Protection Regulation*, di seguito "GDPR") e dal *Regolamento in materia di protezione dei dati personali* (di seguito "Regolamento"), e sia tale in ogni caso da garantire attraverso un trattamento lecito e corretto gli interessi e i diritti fondamentali dell’interessato. Le istruzioni presenti nel documento potranno essere integrate dal titolare del trattamento o dal responsabile interno del trattamento con indicazioni più dettagliate riferite ad uno specifico trattamento.

### Principi guida dell’azione amministrativa

Il diritto alla protezione dei dati personali mira a garantire che il trattamento delle informazioni si svolga “nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell’interessato, con particolare riferimento alla riservatezza, all’identità personale e al diritto alla protezione dei dati personali”. Il principio guida dell’azione amministrativa è rappresentato pertanto dal “principio di necessità del trattamento”, il quale, assieme ai correlati principi di “pertinenza e non eccedenza”, rappresenta un presupposto di liceità del trattamento medesimo. I dati personali oggetto di trattamento devono essere custoditi e controllati, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo, mediante l’adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.

### Livelli adeguati di sicurezza

Nell’ambito del predetto obbligo generale il titolare del trattamento e il responsabile interno del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso

- a) la pseudonimizzazione e la cifratura dei dati personali,
- b) la capacità di assicurare su base permanente la riservatezza<sup>1</sup>, l’integrità<sup>2</sup>, la disponibilità<sup>3</sup> e la resilienza<sup>4</sup> dei sistemi e dei servizi di trattamento,

---

<sup>1</sup> La capacità di garantire l’accesso protetto e controllato ai dati solo alle persone effettivamente autorizzate a garanzia della confidenzialità delle informazioni trattate

<sup>2</sup> La capacità di garantire la consistenza e la protezione dei dati nei confronti di modifiche, accidentali (involontarie) oppure effettuate volontariamente da una terza parte.

<sup>3</sup> La capacità di continuare a trattare dati, nei tempi e nei luoghi previsti, anche a seguito di un incidente o di un evento esterno imprevisto.

- c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico,
- d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

Nel valutare l'adeguato livello di sicurezza, si tiene conto in special modo dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati.

Il titolare del trattamento e il responsabile interno del trattamento fanno sì che chiunque agisca sotto la loro autorità e abbia accesso a dati personali non tratti tali dati se non è istruito in tal senso.

---

<sup>4</sup> La capacità di un sistema di adattarsi alle condizioni d'uso e di resistere all'usura in modo da garantire la disponibilità dei servizi erogati.

## OBBLIGHI

### Trattamento dei dati personali

Il trattamento dei dati personali deve essere effettuato esclusivamente in conformità alle finalità previste e dichiarate dall'Università e alle informazioni che la stessa ha comunicato agli interessati, nonché alle mansioni previste dal contratto di lavoro dell'incaricato. In particolare, devi:

- raccogliere e trattare esclusivamente i dati necessari e sufficienti al corretto svolgimento delle tue proprie mansioni. L'eventuale raccolta dei dati deve avvenire nel rispetto delle procedure e dei modelli di informazione e/o consenso elaborati dall'Università e disponibili nel Regolamento;
- acquisire il consenso dell'interessato laddove previsto;
- garantire all'interessato che ne faccia richiesta l'effettivo esercizio dei diritti previsti dalle vigenti disposizioni in materia di protezione dei dati personali;
- prestare particolare attenzione all'esattezza dei dati trattati e provvedere all'aggiornamento e all'integrazione degli stessi nell'ambito delle proprie attribuzioni;
- provvedere con la dovuta diligenza affinché non vengano conservati dati personali non pertinenti, non necessari o divenuti superflui;
- informare il responsabile interno del trattamento in merito alle richieste degli interessati e supportarlo nella corretta evasione delle stesse, in conformità al Regolamento;
- assicurare che i Responsabili del Trattamento esterni siano vincolati dagli obblighi imposti dal GDPR, adottando le misure contrattuali indicate nel Regolamento e inserendo una clausola a tale scopo nei contratti di fornitura sottoscritti;
- in caso di una violazione che comporta la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali, informare tempestivamente il responsabile interno del trattamento e/o direttamente il responsabile della protezione dei dati e cooperare con lo stesso nella gestione della violazione;
- eseguire esclusivamente le operazioni di trattamento a cui sei autorizzato/a attenendoti alle istruzioni ricevute e alle misure di sicurezza indicate e nel rispetto delle procedure interne dell'Università.

In conclusione, devi utilizzare i dati personali solo per le finalità connesse allo svolgimento delle tue mansioni lavorative, con divieto di qualsiasi altra diversa utilizzazione. 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 personali devono essere trattati nella misura strettamente necessaria e sufficiente per le finalità previste e per il periodo necessario a tali fini. I dati non devono essere comunicati all'esterno dell'Università e comunque a soggetti terzi se non previa autorizzazione.

## Accesso ad archivi cartacei o a banche dati

Le disposizioni e gli obblighi in materia di archivi pubblici sono indifferentemente riferibili ad ogni ente pubblico, pertanto, in base al principio di stretta pertinenza dei trattamenti rispetto alle mansioni svolte, devi:

- accedere esclusivamente agli archivi/banche dati per effettuare i trattamenti strettamente pertinenti alle mansioni svolte e per le finalità previste dal titolare del trattamento, rispettando i principi fondamentali delle regolamentazioni di legge in materia e del Regolamento;
- astenerti dall'accedere ad archivi/banche dati diversi da quelli indicati, nonché realizzare nuove ed autonome banche dati con finalità diverse da quelle consentite (es. laddove compili dei fogli excel con dati di studenti per finalità proprie o comunque diverse da quelle previste per la tua mansione);
- astenerti dal trasportare al di fuori dei luoghi di lavoro i documenti cartacei/ elettronici (o copia degli stessi) senza specifica autorizzazione, salvo i casi di comunicazione dei dati a terzi autorizzati dall'Università;
- impedire che estranei, o in ogni caso terzi non autorizzati, prendano conoscenza dei dati personali non a loro riferibili;
- sviluppare misure idonee a prevenire l'eventuale distruzione, dispersione o accesso non autorizzato ai documenti, e adottando, in presenza di specifici rischi, particolari cautele;
- tutelare l'integrità degli archivi e l'autenticità dei documenti, anche elettronici e multimediali, in particolare di quelli esposti a rischi di cancellazione, dispersione ed alterazione dei dati;
- salvaguardare la conformità delle riproduzioni dei documenti agli originali ed evitare ogni azione diretta a manipolare, dissimulare o deformare fatti, testimonianze, documenti e dati;
- astenerti dal fare alcun uso delle informazioni non disponibili agli utenti o non rese pubbliche, ottenute in ragione della propria attività anche in via confidenziale, per proprie ricerche o per realizzare profitti e interessi privati;
- mantenere riservate i dati personali, notizie e informazioni ad essi concernenti apprese nell'esercizio delle proprie attività, osservando tali doveri di riserbo anche in seguito a modifica dell'incarico e/o cessazione del rapporto di lavoro;
- classificare e fascicolare correttamente tutti i documenti protocollati:
  - a norma dell'art. 52 del DPR 445/2000, il sistema di protocollo informatico deve fornire anche le indicazioni sul collegamento esistente tra ciascun documento ricevuto e i documenti prodotti dall'amministrazione nello svolgimento del relativo procedimento amministrativo, fino all'eventuale provvedimento finale. Il fascicolo informatico è lo strumento che consente l'aggregazione dei documenti all'interno del sistema di protocollo informatico in base al procedimento e nel rispetto del vincolo archivistico;
  - a norma degli artt. 67, 68 e 69 del DPR 445/2000, almeno una volta ogni anno, il Responsabile di ciascuna UOR, provvede a trasferire nell'archivio di deposito tutta la documentazione relativa ai procedimenti conclusi, rispettando l'organizzazione che i fascicoli avevano nell'archivio corrente e i criteri di scarto/conservazione permanente dei documenti, anche al fine di garantire che i dati vengano conservati per il periodo strettamente necessario al conseguimento delle finalità per le quali sono raccolti e trattati

o nei termini previsti da leggi, norme e regolamenti nazionali e comunitari a cui l'Università è tenuta ad attenersi.

## Responsabilità

Ti ricordo che il trattamento dei dati personali effettuato in difformità alle finalità e modalità previste può configurare le ipotesi di responsabilità disciplinate dalla vigente normativa in materia di lavoro e tutela della privacy; pertanto devi:

- compiere tutto quanto sia necessario e adottare tutte le iniziative e gli interventi idonei a garantire il rispetto delle vigenti disposizioni in materia di protezione dei dati personali;
- segnalare tempestivamente ogni eventuale problema relativo all'adempimento degli obblighi previsti dalle vigenti disposizioni in materia di protezione dei dati personali.

Più in generale, dovrai garantire il pieno rispetto delle norme vigenti in materia di trattamento, attenerti alle istruzioni indicate nel Regolamento e ad ogni altra indicazione ricevuta dal titolare del trattamento o dal responsabile per la protezione dei dati.

## ISTRUZIONI OPERATIVE

### Come posso sapere se è consentito compiere un determinato trattamento?

Innanzitutto, assicurati che il trattamento che stai per compiere sia sussumibile sotto uno dei trattamenti indicati nelle informative presenti all'indirizzo <http://www.uniroma3.it/privacy/>.

Se il trattamento è indicato all'interno dell'informativa, puoi procedere con il trattamento in quanto l'Università ha già compiuto le proprie valutazioni in merito all'idonea base giuridica per poter procedere con il trattamento. Se il trattamento che intendi compiere non è indicato tra quelli presenti nelle informative, passa alla prossima domanda.

### Posto che il trattamento non è indicato nelle Informative, posso comunque eseguirlo?

Se un trattamento non è sussumibile sotto uno dei trattamenti indicati nelle informative presenti all'indirizzo <http://www.uniroma3.it/privacy/>, ciò non significa che non possa essere eseguito. Tuttavia, prima di poter cominciare il trattamento sarà necessario (1) individuare l'idonea base giuridica e (2) dare immediata comunicazione del nuovo trattamento al responsabile interno del trattamento e al DPO affinché quest'ultimo possa inserirlo nelle informative sulla protezione dei dati personali pubblicate online dall'Università.

Per individuare l'idonea base giuridica del trattamento occorre distinguere tra dati personali così detti "comuni", dati particolari (o così detti "dati sensibili") e dati relativi a condanne penali, reati o misure di sicurezza (così detti "dati giudiziari"). Fai riferimento alle definizioni contenute nel regolamento di Ateneo per capire in quale categorie rientrano i dati che intendi trattare. Ciò detto, a seconda della categoria, potrai trattare i dati solo se sussiste una delle seguenti condizioni:

- Per quanto concerne i dati personali afferenti alla categoria dei dati "comuni", sussiste una base giuridica per procedere con il trattamento se:
  - il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso (ad esempio, l'interessato è una persona fisica che agisce quale fornitore e il trattamento è necessario per consentire all'Università di adempiere agli obblighi espressamente indicati nel contratto); oppure
  - il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento (ad esempio, c'è una norma di legge che espressamente impone all'Università di eseguire il trattamento); oppure
  - il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica (ad esempio, uno studente, si trova all'estero in una condizione di assoluta emergenza, come un attacco terroristico in corso, e si presume che la sua vita o quella di un'altra persona possa essere in pericolo se non si procede al trattamento, quale, ad esempio, fornire allo stesso dei recapiti telefonici); oppure

- il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento (ad esempio, il trattamento rientra nell'ambito dei servizi di pubblica istruzione che costituiscono vocazione dell'Università, o in altro dei trattamenti individuati espressamente dal Codice Privacy o da altra norma di legge); oppure
- l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità (ad esempio, l'interessato ha fatto una specifica richiesta in tal senso).

Il consenso dell'interessato, quale base giuridica del trattamento, deve essere acquisito solo ed esclusivamente nei casi in cui non sia individuabile una diversa base giuridica per procedere al trattamento.

- Per quanto concerne i dati personali afferenti alla categoria dei dati "sensibili", sussiste una base giuridica per procedere con il trattamento se:
  - il trattamento è necessario per assolvere gli obblighi ed esercitare i diritti specifici del titolare del trattamento o dell'interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale, nella misura in cui sia autorizzato dal diritto italiano, dell'UE o da un contratto collettivo, in presenza di garanzie appropriate per i diritti fondamentali e gli interessi dell'interessato; oppure
  - il trattamento è necessario per tutelare un interesse vitale dell'interessato o di un'altra persona fisica qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso; oppure
  - il trattamento riguarda dati personali resi manifestamente pubblici dall'interessato (da interpretarsi in modo stringente); oppure
  - il trattamento è necessario per accertare, esercitare o difendere un diritto in sede giudiziaria dinanzi una autorità con funzioni giurisdizionali; oppure
  - il trattamento è necessario per motivi di interesse pubblico rilevante sulla base del diritto italiano o del diritto UE, che deve essere proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato; oppure
  - il trattamento è necessario per finalità di medicina preventiva o di medicina del lavoro, valutazione della capacità lavorativa del dipendente, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali sulla base del diritto italiano o dell'UE; oppure
  - il trattamento è necessario a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, secondo quanto previsto dal diritto italiano o dell'UE, che è proporzionato alla finalità perseguita, rispetta l'essenza del diritto alla protezione dei dati e prevede misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato; oppure
  - l'interessato ha prestato il proprio consenso esplicito al trattamento di tali dati personali per una o più finalità specifiche, salvo che la normativa disponga comunque che detto trattamento non possa compiersi.

Il consenso dell'interessato, quale base giuridica del trattamento, deve essere acquisito solo ed esclusivamente nei casi in cui non sia individuabile una diversa base giuridica per procedere al trattamento.

- Per quanto concerne i dati personali afferenti alla categoria dei dati "giudiziari", sussiste una base giuridica per procedere con il trattamento se:
  - il trattamento è espressamente autorizzato dal diritto italiano o dell'UE, e tale norma prevede garanzie appropriate per i diritti e le libertà degli interessati. Se tale base giuridica si fonda su un'autorizzazione generale del Garante per la protezione dei dati personali, dovrà scrupolosamente accertarsi che detta autorizzazione sia vigente e applicabile al caso concreto. Inoltre, si ricorda che il trattamento dei dati "giudiziari" non può trovare fondamento nel meccanismo del consenso.

Una volta individuata la pertinente base giuridica del trattamento, tenendo conto delle indicazioni sopra fornite e della normativa applicabile, si prega di informare tempestivamente il proprio responsabile interno del trattamento e il DPO, affinché quest'ultimo possa darne menzione nelle informative di cui all'indirizzo <http://www.uniroma3.it/privacy/>.

### Cosa fare se dati personali sono stati sottratti, comunicati o diffusi a persone terze non autorizzate?

Devi eseguire scrupolosamente la *procedura di notifica della violazione di dati personali* descritta nel Regolamento.

### Conserva sempre il consenso rilasciato dall'interessato

Laddove sia necessario raccogliere il consenso, occorre predisporre misure organizzative e tecniche atte a garantire la conservazione della copia del consenso acquisito, sia esso cartaceo o elettronico, da parte della struttura autorizzata al trattamento; in particolare:

- il consenso richiede una dichiarazione o un'azione positiva inequivocabile da parte dell'interessato, il che significa che il consenso deve sempre essere espresso attraverso una dichiarazione o in modo attivo. Pertanto è vietato predisporre moduli in cui la casella di acquisizione del consenso (c.d. "check-box") risulta pre-compilata con lo specifico simbolo (c.d. flag),
- qualora il consenso sia espresso in formato elettronico è opportuno memorizzare quante più informazioni utili relativamente all'operazione eseguita dall'interessato: data e ora, indirizzo IP di provenienza, sistema operativo e nome utente, ecc.,
- qualora il consenso sia espresso in formato cartaceo occorre conservare la copia cartacea per la durata utile del trattamento e oltre la cessazione del trattamento ove previsto da regolamenti di ateneo o dalla normativa vigente.

### Gestisci la distanza di cortesia

Il ricevimento degli utenti va organizzato in modo da evitare che persone terze, dipendenti o meno, possano, anche involontariamente, ascoltare i colloqui che ciascun utente intrattiene con il personale

addetto a recepire le relative istanze. Deve, cioè, essere garantita la così detta *distanza di cortesia* nelle ipotesi in cui vengano in rilievo dati personali dell'interessato.

### Non comunicare dati personali a soggetti non legittimati

L'utilizzo dei dati personali deve avvenire in base al così detto "principio di necessità", è cioè essi non devono essere condivisi, comunicati o inviati a persone che non ne necessitano per lo svolgimento delle proprie mansioni lavorative. I dati non devono essere comunicati all'esterno dell'Università e comunque a soggetti terzi, se non previa autorizzazione del responsabile interno del trattamento nelle ipotesi consentite dalla normativa vigente.

### Utilizza le chiavi

Il primo livello di protezione di qualunque sistema è quello fisico; è vero che una porta chiusa può in molti casi non costituire una protezione sufficiente, ma è anche vero che pone, se non altro, un primo ostacolo e richiede comunque uno sforzo volontario non banale per la sua rimozione.

È fin troppo facile per un estraneo entrare in un ufficio non chiuso a chiave e sfogliare i documenti posti su una scrivania; pertanto:

- chiudi a chiave il tuo ufficio quando l'ultima unità di personale lascia il locale,
- non lasciare i documenti incustoditi sul tavolo, ma riponili in fascicoli non immediatamente accessibili,
- alla fine della giornata chiudi i documenti a chiave nei cassetti o negli armadi ogni volta che puoi.

### Cura la spedizione dei documenti

Il trasferimento di ogni documento contenente dati personali deve seguire rigorose misure di garanzia, tali da impedire che allo stesso accedano estranei: buste chiuse e sigillate, invio con raccomandata di ritorno, non abbandono durante i trasferimenti.

Tali accortezze possono essere ridotte qualora si utilizzi il servizio postale interno all'Università; resta comunque valida l'accortezza di imbustare i documenti per non renderli immediatamente accessibili.

### Conserva i documenti cartacei nel modo corretto

Esamina le modalità di archiviazione delle informazioni valutando se ne hai ancora bisogno e se il luogo di conservazione permette l'accesso solo al personale autorizzato.

I documenti da conservare devono essere gestiti in modo da poter essere rintracciati e individuati facilmente, se necessario. I documenti contenenti dati sensibili devono essere conservati in armadietti chiusi a chiave il cui accesso è limitato a un determinato numero di persone all'interno dell'Università.

### Fai attenzione a come distruggi i documenti

Qualora sia necessario distruggere i 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. Anche eventuali fotocopie mal riuscite di documenti contenenti dati

personali devono essere distrutte. I documenti originali non possono in alcun caso essere distrutti senza la previa autorizzazione della Soprintendenza Archivistica.

### Non lasciare in vista documenti

In caso di riunione nella tua stanza, di ricevimento di utenti o ancora se lavori presso uno sportello informativo, fai sempre attenzione ai documenti presenti sulla tua postazione di lavoro.

Assicurati di rimuoverli e di archivarli per tempo per evitare che chiunque possa accedere a informazioni personali.

### Raddoppia le attenzioni se i documenti contengono dati particolarmente sensibili

I documenti contenenti dati particolarmente sensibili devono essere controllati e custoditi molto attentamente in modo che non vi accedano persone prive di autorizzazione. Ad esempio, la consultazione di certificati medici, permessi sindacali, condanne penali, ecc., deve avvenire per il tempo strettamente necessario e, subito dopo, i documenti devono essere archiviati.

L'archiviazione dei documenti cartacei deve avvenire possibilmente in locali ad accesso controllato, utilizzando armadi o contenitori chiusi a chiave. Per accedere agli archivi fuori dall'orario di lavoro è necessario ottenere una preventiva autorizzazione oppure farsi identificare e registrare su appositi registri.

### Non dimenticare le stampe dei documenti

Stampare un documento e dimenticarsi di averlo fatto può costituire un rischio per la sicurezza. Non lasciare accedere alle stampe o ai fax persone non autorizzate; se la stampante o il fax non si trova sulla tua scrivania recati quanto prima a ritirare le stampe.

Sincerati inoltre che al momento dello spegnimento del computer non vi siano documenti in coda di stampa.

### Limita l'uso di supporti di memorizzazione portatili

I supporti di memorizzazione portatili, quali CD, DVD, chiavette USB, dischi esterni, ecc. rappresentano un potenziale rischio per la perdita dei dati. Difatti qualora vengano smarriti o sottratti chiunque vi acceda può comunicare o diffondere dati personali a persone terze non autorizzate. È pertanto fortemente consigliato utilizzare i sistemi di comunicazione, memorizzazione e condivisione dei dati messi a disposizione dall'Università quali la posta elettronica, OneDrive, Filesender e SharePoint<sup>5</sup>. Per i supporti di memorizzazione elettronica si applicano gli stessi criteri dei documenti cartacei: riponeteli negli armadi o nei cassette non appena avete finito di usarli e non lasciateli incustoditi sul tavolo.

### La password è personale

La password o i dispositivi di autenticazione (badge, dispositivi OTP, cellulare, ecc.) sono strettamente personali e non devono essere a conoscenza o prestati a nessun altro utente all'infuori del proprietario. Se

---

<sup>5</sup> Si rimanda all'appendice per la descrizione di tali strumenti.

hai il sospetto che qualcuno possa essere venuto a conoscenza della tua password, cambiala immediatamente.

### Non comunicare mai la tua password a seguito di una mail

Spesso succede di ricevere messaggi di posta elettronica, SMS o comunicazioni social, nelle quali un malintenzionato cerca di ingannare la vittima convincendola a fornire informazioni personali, dati finanziari o codici di accesso, fingendosi un ente affidabile quale una banca, un fornitore di servizi informatici o addirittura un collega di lavoro. Il messaggio imita nell'aspetto e nel contenuto messaggi legittimi e richiede di fornire soldi o informazioni riservate come, ad esempio, il numero della carta di credito o la password per accedere ad un determinato servizio.

Ricorda che nessuno è autorizzato a conoscere la tua password, neanche i tecnici informatici e tantomeno a chiedertela tramite posta elettronica: non rispondere per alcun motivo al messaggio e cancellalo.

### Utilizza le password in modo corretto

Vi sono differenti categorie di password, ognuna con il proprio ruolo preciso:

- la password di accesso al computer impedisce l'utilizzo improprio della tua postazione, quando per un motivo o per l'altro non ti trovi in ufficio,
- la password di accesso alla rete impedisce che l'eventuale accesso non autorizzato a una postazione renda disponibili tutte le risorse dell'Ufficio,
- la password dei programmi specifici permette di restringere l'accesso ai dati al solo personale autorizzato,
- la password del salvaschermo, infine, impedisce che una tua assenza momentanea permetta a una persona non autorizzata di visualizzare il tuo lavoro.

Imposta o chiedi ai tecnici informatici che venga sempre impostata una password.

### Blocca sempre i dispositivi informatici quando non li utilizzi

Ogni qual volta devi sospendere il lavoro sullo strumento informatico, assicurati che lo stesso sia bloccato e che non vi si possa accedere se non digitando la relativa password o PIN.

### Non farti sbirciare quando digiti le password

Anche se molti programmi non ripetono in chiaro la password sullo schermo, quando digiti la tua password, questa potrebbe essere letta guardando i tasti che stai battendo sulla tastiera, anche se hai buone capacità di dattiloscrittura. Assicurati che non ci sia nessuno nelle vicinanze che possa carpire la password.

Analogamente sui dispositivi touch (tablet, smartphone, ecc.) il codice PIN digitato per lo sblocco del dispositivo o la password possono essere facilmente individuati a partire dalle porzioni dello schermo sulle quali si depositano le impronte. Per ridurre il rischio, pulisci spesso lo schermo e sostituisci frequentemente la pellicola salvaschermo.

### Custodisci le password in un luogo sicuro

Non scrivere la tua password, meno che mai vicino alla tua postazione di lavoro. L'unico dispositivo di registrazione affidabile è la tua memoria. Se hai necessità di conservare traccia delle password per scritto, non lasciare in giro i fogli utilizzati.

Applica lo stesso criterio anche per le credenziali di firma elettronica dei documenti.

### Scegli bene la tua password

Il più semplice metodo per l'accesso illecito a un sistema consiste nell'indovinare la password dell'utente legittimo. In molti casi sono stati procurati seri danni al sistema informativo a causa di un accesso protetto da password "deboli". La scelta di password "forti" è parte essenziale della sicurezza informatica. Utilizza password che sia per te facile da ricordare (legata ad esempio alla vita personale non conosciuta dagli altri) che abbia le seguenti caratteristiche:

- deve essere obbligatoriamente cambiata almeno ogni 3/6 mesi,
- lunghezza minima di otto caratteri (consigliata almeno 12),
- deve contenere almeno una lettera maiuscola,
- deve contenere almeno una lettera minuscola,
- deve contenere almeno un numero,
- deve contenere almeno un carattere speciale (es \$, #, ?, !, ecc.),
- deve essere diversa dalle ultime tre utilizzate.

### Per ogni account usa password differenti

Non utilizzate mai la password della mail per altri account, ad esempio quelli social; qualora venisse violata la password del profilo social i truffatori avrebbero l'accesso anche alla tua mail. Per quanto possibile utilizza password diverse per ogni servizio on-line cui sei registrato.

### Cosa non devi fare con la tua password

- NON dire a nessuno la tua password. Ricorda che lo scopo principale per cui utilizzi una password è assicurare che nessun altro possa utilizzare le tue risorse o possa farlo a tuo nome. Non comunicarla neanche ai tecnici informatici incaricati dell'assistenza sul tuo pc e ove assolutamente indispensabile, procedi immediatamente dopo a cambiarla,
- NON usare il tuo nome o cognome: è la password più semplice da indovinare,
- NON usare password che possano in qualche modo essere legate a te che possono essere facilmente conosciute come, ad esempio, il nome del coniuge o dei figli, del cane, date di nascita, numeri di telefono ecc.

### Presta attenzione all'utilizzo dei personal computer portatili o tablet

I personal computer portatili e i tablet sono un facile bersaglio per i furti. Se hai necessità di gestire dati riservati su un portatile, chiedi l'installazione di un buon programma di cifratura del disco rigido oppure utilizza i sistemi di comunicazione, memorizzazione e condivisione dei dati messi a disposizione dall'Università quali la posta elettronica, OneDrive, Filesender e SharePoint in modo da limitare i dati personali sul dispositivo.

### Non utilizzare dispositivi non autorizzati

I dispositivi di accesso (computer, tablet, smartphone, modem, ecc.) rappresentano un punto di accesso sia alla rete che ai dati trattati. Pertanto, è necessario che su di essi vengano applicate le misure minime previste al fine di garantirne la sicurezza e l'integrità. L'utilizzo di dispositivi personali o non autorizzati viola le politiche di sicurezza definite dall'Università; ad esempio:

- l'utilizzo di modem o di hot-spot wi-fi su postazioni di lavoro collegati alla rete dell'Università offre una porta d'accesso dall'esterno non solo al vostro computer, ma a tutta la rete, ed è quindi vietata,
- l'utilizzo di computer personali o di supporti di memorizzazione portatili personali (chiavette usb, dischi esterni, CD, ecc.) può rappresentare un veicolo per la diffusione di virus e la conseguente perdita di dati.

### Non installare programmi non autorizzati

Solo i programmi istituzionali o acquistati dall'Università con regolare licenza sono autorizzati. Se il tuo lavoro richiede l'utilizzo di programmi specifici, consulta i tecnici autorizzati ad effettuare l'assistenza sul tuo PC.

### Non utilizzare strumenti di comunicazione, memorizzazione e condivisione non autorizzati

Oggi è facile creare account "personali" per usufruire di servizi di comunicazione (es Gmail, Yahoo Mail, Hotmail, ecc.), di memorizzazione e condivisione (GoogleDrive, Dropbox, WeTransfer, ecc.). Si tratta appunto di account "personali" legati alla propria persona e in fase di attivazione del servizio il fornitore non ha alcun obbligo di riservatezza in riferimento a dati che non riguardano colui che ha attivato l'account. A ciò si aggiunge che, per rispettare quanto previsto dal GDPR, il fornitore del servizio deve essere nominato responsabile del trattamento. Pertanto, trasferire su tali sistemi dati personali riguardanti, ad esempio, dati anagrafici degli studenti, rappresenta una violazione delle norme sulla privacy.

È pertanto vietato:

- inoltrare la posta elettronica ricevuta sull'indirizzo istituzionale ([xxxx@uniroma3.it](mailto:xxxx@uniroma3.it) o [xxx@yyy.uniroma3.it](mailto:xxx@yyy.uniroma3.it)) verso altri indirizzi di posta elettronica (ad esempio privati, o di aziende presso le quali si sta svolgendo contemporaneamente altra attività lavorativa),
- memorizzare o condividere file utilizzando piattaforme (ad esempio GoogleDrive, Dropbox, WeTransfer, ecc.) diverse da quelle istituzionali.

### Applica con cura le linee guida per la prevenzione da infezioni di virus

La prevenzione dalle infezioni da virus sul vostro computer è molto più facile e comporta uno spreco di tempo molto minore della correzione degli effetti di un virus; tra l'altro, potreste incorrere in una perdita irreparabile di dati o nella divulgazione di dati personali a terzi.

### Diffida delle mail sospette

Diffida dalle mail che contengono fatture di servizi, prodotti mai acquistati o documenti provenienti dalla pubblica amministrazione senza posta certificata. Se hai effettuato un acquisto, attendi una spedizione o una fattura ma l'email sembra sospetta, contatta direttamente il fornitore per verificarla.

Contrassegna l'email di phishing come posta indesiderata, in questo modo futuri invii dello stesso tipo saranno intercettati automaticamente e non ti saranno riproposti.

### Non utilizzare la mail istituzionale per la registrazione a servizi personali

L'email malevole possono anche non avere dei fini economici diretti, in molti casi vengono inviate anche solo per prendere il controllo del vostro pc, per utilizzarlo a vostro nome per effettuare altri attacchi o accedere all'interno di una rete. Per questo non dovete utilizzare la vostra mail istituzionale per iscrivervi a servizi on-line di e-banking, e-commerce, ai social network, forum e blog; esponete l'Università e i vostri dati a nuovi rischi.

### Fai attenzione a come distruggi i supporti di memorizzazione

I supporti di memorizzazione (chiavette usb, dischi esterni, CD, DVD, dischi rigidi, ecc.) contenenti dati personali devono essere cancellati in modo definitivo prima di essere ceduti a terzi o smaltiti.

La semplice cancellazione dei file (ad esempio effettuata con il tasto "CANC") da un supporto di memoria o la formattazione di un hard disk non significa che le informazioni registrate siano cancellate per sempre. Spesso, queste ultime rimangono fisicamente presenti e tecnicamente recuperabili. Inoltre, bisogna considerare che dati personali possono essere contenuti anche in apparecchi elettronici apparentemente insospettabili: ad esempio, le moderne fotocopiatrici, i fax e le stampanti sono dotate di un hard disk interno simile a quello che si trova nei PC e nei laptop. Questi apparecchi memorizzano automaticamente qualsiasi documento che sia stato fotocopiato o stampato e possono quindi contenere dati personali da distruggere al momento della loro dismissione o reimpiego.

Qualora non sia possibile cancellare in modo permanente i dati da un dispositivo, questo deve essere distrutto.

### Ricordati di fare sempre il backup

I dati possono essere cancellati per diverse cause: involontariamente, con l'esecuzione di operazioni errate, a causa di virus, a seguito di furto, per verificarsi di calamità naturali, ecc. Per tale motivo chi dispone di dati personali su supporto informatico deve provvedere periodicamente ad eseguire le cosiddette copie di salvataggio (backup) delle informazioni che si intende proteggere da indebita o volontaria cancellazione. Il salvataggio dei dati va effettuato con cadenza almeno settimanale ed è obbligatorio qualora i dati in questione non siano disponibili presso altri sistemi informatici. Difatti l'Università è tenuta al ripristino dell'accesso ai dati in caso di danneggiamento degli stessi, in tempi certi compatibili con i diritti degli interessati. Si consiglia quindi l'utilizzo di strumenti di memorizzazione messi a disposizione dall'Università.

### Dove puoi posizionare i server

Nel caso di trattamento informatico, devono essere attivate, se non già operative, procedure di controllo d'accesso alle sale in cui sono ubicati server e ai locali dove sono ubicati gli altri sistemi informatici utilizzati per il trattamento di dati personali. Evitate di installare server che contengono dati personali all'interno della propria stanza o in zone facilmente accessibili a chiunque.

## ISTRUZIONI OPERATIVE PER IL WEB

### Cancella fisicamente i file dal server web

Ricordati che i file pubblicati, seppur non più collegati all'interno della pagina web, sono sempre raggiungibili dai motori di ricerca. Ricordati quindi di cancellare fisicamente i file dal server e non limitarti a rimuovere semplicemente il link dalla pagina.

### Non pubblicare gli esiti degli esami

Non pubblicare esiti degli esami o delle prove intermedie. Per pubblicare queste informazioni, utilizza il sistema di gestione delle carriere degli studenti che consente di pubblicare o inviare comunicazioni solo ai diretti interessati.

### Limita le informazioni pubblicate nelle graduatorie

Qualora sia necessario pubblicare dati personali sul web utilizza per quanto possibile sistemi che consentano l'accesso alle informazioni solo attraverso le credenziali di autenticazione che hanno tutte le studentesse, gli studenti e il personale. Se proprio non è possibile utilizzare questi strumenti, ove non sussistano altre norme di pubblicità o trasparenza, limitati a pubblicare solo il cognome e nessun'altro dato personale (nome, data, luogo di nascita, codice fiscale, ISEE, IBAN, dati di domicilio/residenza, recapiti telefonici/email, ecc.).

Se è proprio necessario caricare ulteriori dati personali, contatta il responsabile interno del trattamento per definire le modalità di pubblicazioni e quali informazioni devono prima essere oscurate.

In ogni caso rimuovi fisicamente il file pubblicato sul web una volta che non è più necessario ai fini del procedimento che si è concluso.

Ricordati inoltre che:

- nel d.lgs. 33/2013, come modificato dal d.lgs. 97/2016, sono contenute specifiche indicazioni sull'attuazione degli obblighi di pubblicità, trasparenza e diffusione di informazioni,
- sul sito del Garante sono pubblicate le [Linee guida per il trattamento di dati personali effettuato da soggetti pubblici per finalità di pubblicazione e diffusione sul web](#) che rappresentano un utile riferimento nell'individuare contenuti, modalità ed eccezioni relativamente alla pubblicazione di dati personali sul web.

### Non pubblicare mai documenti con le firme autografe

Per garantire l'accessibilità dei documenti pubblicati, anche da persone con disabilità, è indispensabile pubblicare il file originario (word, excel, ecc.) convertito in formato pdf. Un documento di testo acquisito mediante scansione, anche se in formato pdf, è inaccessibile e pertanto non deve essere pubblicato. Eventualmente al documento originario, prima di essere convertito in pdf, può essere aggiunta l'indicazione (F.to) accanto al nominativo del firmatario – ad esempio (F.to) Mario Rossi – o la dicitura: "Il presente documento, conforme all'originale, è conservato negli archivi ...", indicando l'ufficio competente alla conservazione del documento stesso.

Non devono essere mai pubblicati documenti contenenti firme autografe o la scansione di firme autografe.

## ISTRUZIONI OPERATIVE PER LA VIDEO SORVEGLIANZA

Tutte le immagini che contengono informazioni relative a persone fisiche e ne consentono l'identificazione anche indirettamente o mediante riferimenti sono classificate "DATI PERSONALI". Pertanto, in materia di videosorveglianza, la consultazione, la conservazione, l'estrapolazione, la manipolazione e la cancellazione, sono tutte operazioni che costituiscono un trattamento di dati.

Il personale autorizzato che ha accesso alle immagini in diretta o registrate ha l'obbligo di mantenere riservati i dati durante ciascuna operazione di trattamento.

### Posiziona correttamente il cartello

Il cartello "informativa" deve essere accessibile e chiaramente visibile a tutti gli interessati rispettando determinate caratteristiche: esso deve essere posizionato prima del raggio di azione della telecamera o nelle sue immediate vicinanze, non necessariamente a contatto con gli impianti. Deve essere chiaramente visibile e riconoscibile mediante il suo formato e collocamento, in ogni condizione di illuminazione ambientale, anche in orario notturno.

### Limita la visuale di ripresa

Il trattamento di dati mediante l'uso delle apparecchiature volte a riprendere ("Telecamere"), con o senza registrazione delle immagini, deve essere effettuato con modalità tali da limitare l'angolo visuale all'area effettivamente da proteggere, evitando, per quanto possibile, la ripresa di luoghi circostanti per non incorrere nel reato penale di "Interferenze illecite nella vita privata". Resta anche vietato l'utilizzo di telecamere finte.

### Proteggi i monitor e i registratori

Il monitor di controllo presente presso i siti videosorvegliati o in una sala operativa centralizzata, deve essere posizionato in un luogo sicuro, presidiato e in modo da non consentire che terzi possano sbirciare, fotografare o video-riprendere le immagini rappresentate su di esso.

Le modalità di protezione dei DVR/NVR sono le medesime utilizzate per i server che trattano dati personali. È altresì necessario adottare le misure di sicurezza preventive come password complesse, crittazione dei dati e altri strumenti disponibili, durante i processi di conservazione e manipolazione delle immagini.

### Cancella i supporti

Inoltre, prima della dismissione dei dispositivi e comunque in tutti i casi ove la presenza delle immagini non sia più utile, è importante accertarsi che i supporti di memorizzazione siano stati cancellati definitivamente e i filmati siano irrecuperabili.

### La diffusione è vietata

I dati personali relativi alla videosorveglianza possono essere utilizzati esclusivamente per quelle che sono le finalità per cui è stato attivato il trattamento. È assolutamente vietato darne diffusione a soggetto alcuno, anche se dipendente dell'Università, ad eccezione dei dati ceduti su specifico ordine, alle Autorità Giudiziarie a fini investigativi.

## ISTRUZIONI OPERATIVE PER I SOCIAL NETWORK

Per Social Network, si intende un gruppo di persone connesse tra di loro sia a livello umano che a livello virtuale attraverso “piattaforme sociali” il cui scopo principale è la conoscenza, lo scambio di informazioni, di risorse e quant’altro. Tra le più utilizzate a livello mondiale possiamo citare: Facebook, Twitter, Instagram e LinkedIn.

### L’identificazione non è sicura

Non comunicare attraverso i social informazioni personali, ma utilizza sempre gli strumenti ufficiali dell’Università per identificare il destinatario della comunicazione (posta elettronica di ateneo, cellulare di servizio). L’interlocutore si potrebbe celare dietro false identità per carpire in modo illegittimo dati personali altrui. Identifica l’interessato esclusivamente con sistemi basati sul riconoscimento diretto o sicuro prima dar seguito alle sue richieste.

### Non pubblicare alcun dato personale

La pubblicazione di dati personali (elenchi nominativi, voti, valutazioni didattiche, foto, filmati, pensieri ecc.) è irreversibile. Nonostante la volontà di rimuoverli dai social, i contenuti, se già diffusi, resteranno illimitatamente nella rete. Prima di condividere qualsiasi dato, riferito a soggetti terzi o a te stesso, fai la massima attenzione. Evita che i dati personali possano finire nelle mani sbagliate.

### Disattiva la Geo-localizzazione

Per quanto ormai diffusa la moda di postare nei social, foto, video, posizione geocartografica dei luoghi che visitiamo, è consigliato farlo solo nella fase successiva al rientro dal viaggio, in modo da evitare che eventuali malfattori, a conoscenza dell’assenza dall’abitazione e dal luogo di lavoro, possano approfittarne per commettere azioni criminose ed entrare in possesso oltre che di oggetti, documenti o dispositivi che contengono i dati personali propri o altrui.

## ISTRUZIONI OPERATIVE PER LA PREVENZIONE DEI VIRUS

Un virus è un programma in grado di trasmettersi autonomamente e che può causare effetti dannosi. Alcuni virus si limitano a “riprodursi” senza ulteriori effetti, altri si limitano alla semplice visualizzazione di messaggi sul video, i più dannosi arrivano a distruggere tutto il contenuto del disco rigido.

Come si trasmette un virus:

- attraverso l’installazione di programmi provenienti da fonti non ufficiali o non autorizzate,
- attraverso la copia di dati da supporti di memorizzazione (USB, hard disk, ecc.),
- attraverso le macro presenti nei file dei programmi di automazione d’ufficio (Office, OpenOffice, ecc.),
- attraverso dati o programmi che si scaricano da Internet.

Come non si trasmette un virus:

- attraverso file di dati non in grado di contenere macro (file di testo, html, pdf, ecc.),
- attraverso mail non contenenti allegati.

Come prevenire i virus:

1. usa soltanto programmi provenienti da fonti fidate: copie sospette di programmi possono contenere virus o altro software dannoso. Ogni programma deve essere sottoposto alla scansione prima di essere installato. Non utilizzate programmi non autorizzati,
2. evita di collegare al tuo computer supporti di memorizzazione (USB, hard disk, ecc.): infatti se il supporto di memorizzazione fosse infettato, il virus si trasferirebbe nel computer e potrebbe contagiare ad altri file,
3. proteggi i tuoi supporti di memorizzazione da scrittura quando possibile: in questo modo eviterai le scritture accidentali, magari tentate da un virus. I virus non possono in ogni caso aggirare la protezione meccanica,
4. assicurati che il tuo software antivirus sia aggiornato: la tempestività nell’azione di contrasto è essenziale per limitare i danni che un virus può causare ed è pertanto è vitale che il programma antivirus sia aggiornato e che conosca gli ultimi aggiornamenti sulle “impronte digitali” dei nuovi virus. Gli aggiornamenti sono rilasciati, di solito, con frequenza almeno giornaliera,
5. non diffondere messaggi di provenienza dubbia: se ricevi messaggi che avvisano di un nuovo virus pericolosissimo, ignoralo: messaggi di questo tipo sono detti con terminologia anglosassone *hoax* (termine spesso tradotto in italiano con “bufala”),
6. non partecipare a “catene di s. antonio” e simili: tutti i messaggi che vi invitano a “diffondere la notizia quanto più possibile” sono *hoax*, aventi spesso scopi molto simili a quelli dei virus, cioè utilizzare indebitamente le risorse informatiche.

Per qualsiasi dubbio, o per ulteriori informazioni, prima di installare qualsiasi programma o aprire qualsiasi mail sospetta, contatta i tecnici autorizzati ad effettuare l’assistenza sul tuo computer.

## INFORMAZIONI SUGLI STRUMENTI DI COLLABORAZIONE DISPONIBILI

L'Ateneo mette a disposizione dei suoi utenti (studenti e personale) strumenti di collaborazione per la condivisione di informazioni, quali:

- Filesender: applicazione web per l'invio facile e sicuro di file di grandi dimensioni,
- FindTime: piattaforma per confrontare le disponibilità e trovare l'orario migliore per organizzare una riunione (un servizio analogo a Premium Doodle),
- IBM Connections: piattaforma con una serie di strumenti (blog, chat, forum, wiki, profili, like e commenti) che aumentano l'efficienza comunicativa e collaborativa tra colleghi
- OneDrive: spazio disco da 5 TB per la gestione di documenti con gruppi di lavoro (un servizio analogo a DropBox, GoogleDrive, ecc),
- Outlook: casella di posta elettronica da 100 GB,
- SharePoint: ambiente di collaborazione per la condivisione di documenti, attività, processi, etc.,
- Skype: strumento di comunicazione e collaborazione per realizzare chat, video conferenze anche contemporaneamente con più utenti (di ateneo o di altre organizzazioni) dalla propria postazione di lavoro o con il proprio smartphone,
- Yammer: piattaforma di Social Network dedicata per personale universitario e studenti.

L'impiego di questi strumenti aumenta la sicurezza dei dati, pertanto per quanto possibile utilizzali. Di seguito trovi le informazioni sui alcuni di questi strumenti, per qualsiasi ulteriore delucidazione puoi contattare i tecnici informatici incaricati dell'assistenza sul tuo pc.

### Filesender

Si tratta di un'applicazione web che permette agli utenti di inviare a qualsiasi destinatario, in modo facile e sicuro, file molto grandi ovviando ai limiti solitamente imposti alla posta elettronica.

I file inviati vengono caricati su un'area di storage temporanea e restano disponibili per il download per un periodo di tempo limitato, dopodiché vengono automaticamente cancellati. La sicurezza è garantita perché solo i legittimi destinatari sono in grado di scaricare i file: ogni volta che verrà scaricato, al mittente verrà inviata una notifica via e-mail. È possibile inviare file a qualsiasi indirizzo di posta elettronica, anche non universitario. Il servizio permette anche la ricezione di file da utenti non in possesso delle credenziali di ateneo, o di una università o ente federato in IDEM.

Il servizio può essere utilizzato solo per l'invio di file e non costituisce una piattaforma di storage o di pubblicazione permanente. FileSender è utilizzabile da tutti gli utenti delle organizzazioni aderenti alla Federazione GARR (Università ed Enti di Ricerca).

Per utilizzare FileSender GARR basta collegarsi all'indirizzo: <https://filesender.garr.it> selezionare il nome dell'organizzazione (Università degli studi Roma Tre) ed effettuare il login con le credenziali di ateneo.

## OneDrive

OneDrive è un servizio di *file hosting* sviluppato da Microsoft che connette l'utente a tutti i file. Consente di archiviare in un'unica posizione i tuoi file personali fino ad 1 TB, condividerli con altri utenti (interni od esterni all'Università) e accedervi ovunque si trovino in tutti i dispositivi.

Tutti i file archiviati in OneDrive sono privati a meno che non decidi di condividerli. È possibile condividere file e cartelle con i colleghi in modo da poter collaborare ai progetti, ma anche con partner esterni all'Università. Quando si inviano messaggi di posta elettronica dalla webmail, è possibile allegare un file di OneDrive come collegamento, invece di inviare il file vero e proprio: in questo caso è possibile assegnare automaticamente ai destinatari del messaggio l'autorizzazione per la modifica o meno del file e la data sino alla quale il file resterà disponibile.

È inoltre possibile sincronizzare il contenuto di OneDrive su diversi dispositivi in modo da accedere ai file in piena mobilità: ad oggi è possibile collegare dispositivi con sistema operativo Windows, MacOS, Android o iOS.

OneDrive conserva automaticamente la cronologia di tutte le revisioni effettuate sui file, pertanto è possibile ripristinare le versioni precedenti. Inoltre OneDrive rappresenta un backup dei propri file: difatti in caso di furto, distruzione o sostituzione del proprio dispositivo è possibile recuperare tutti i file dal cloud.

## Outlook

L'Università mette a disposizione un servizio cloud di posta elettronica: oltre alle normali funzioni di ricezione e invio della posta, è possibile i calendari degli altri utenti per pianificare le riunioni, prenotare le sale riunioni, programmare video conferenze.

## Sharepoint

SharePoint è una piattaforma software di Content Management System (CMS) sviluppata da Microsoft, ovvero permette la creazione di siti web principalmente ad uso interno per condividere documenti e altre informazioni. È possibile creare liste, repository documentali, attività, calendari sincronizzati con Outlook e altro. Dal momento che tutte le informazioni sono salvate su server, è possibile lavorare su di essi in collaborazione, ricevere notifiche ogni qual volta un utente ha modificato un file, condividere commenti e post, definire workflow di approvazione, ricercare documenti, il tutto assegnando a ciascun gruppo di utenti profili differenti (utenti che possono solo visualizzare, oppure modificare i contenuti, ecc).

Si tratta quindi di uno strumento che aggiunge alle funzionalità di condivisione dei file (già presenti in OneDrive) ulteriori funzionalità che consente l'interazione e la collaborazione tra utenti.