

UNIVERSITÀ TELEMATICA INTERNAZIONALE UNINETTUNO

# Linee guida per i controlli e la sicurezza dei beni aziendali

(Regolamento UE 2016/679)

UTIU

01/12/2023

**SOMMARIO**

- 1 - RIFERIMENTI NORMATIVI ..... 2**
  - Scopo e ambito di applicazione..... 2
  - Definizioni..... 3
  
- 2 - INDIVIDUAZIONE DEGLI STRUMENTI DI LAVORO..... 5**
  - Strumenti utilizzati dal lavoratore..... 5
  - Strumenti di registrazione degli accessi e delle presenze..... 6
  
- 3 - MODALITÀ DI UTILIZZO DEGLI STRUMENTI DI LAVORO E DELLE ATTIVITÀ DI CONTROLLO PER ESIGENZE DI SICUREZZA E PROTEZIONE DEL PATRIMONIO AZIENDALE..... 8**
  - uso del pc e dei dispositivi portatili ..... 8
  - uso dei programmi applicativi..... 8
  - uso dei servizi di navigazione web e posta elettronica..... 9
  - uso degli strumenti di formazione a distanza .....11
  - uso degli strumenti di lavoro manuali .....12

# 1 - RIFERIMENTI NORMATIVI

## SCOPO E AMBITO DI APPLICAZIONE

L'UNIVERSITÀ TELEMATICA INTERNAZIONALE UNINETTUNO (in breve UTIU) in qualità di Titolare del trattamento ha l'obbligo legale di mettere in atto misure tecniche e organizzative adeguate, allo scopo di garantire ed essere in grado di dimostrare in caso di necessità che il trattamento di dati personali effettuato dalla stessa sia conforme ai principi e ai doveri stabiliti dal Regolamento UE 2016/679, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati.

Nella sua qualità di datore di lavoro è inoltre tenuta a garantire il rispetto della dignità e la libertà dei lavoratori previsto dall'art. 4 della legge n. 300/1970, di cui si riporta di seguito il testo:

*“Art. 4. Impianti audiovisivi.*

- 1. Gli impianti audiovisivi e gli altri strumenti dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori possono essere impiegati esclusivamente per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale e possono essere installati previo accordo collettivo stipulato dalla rappresentanza sindacale unitaria o dalle rappresentanze sindacali aziendali. In alternativa, nel caso di imprese con unità produttive ubicate in diverse province della stessa regione ovvero in più regioni, tale accordo può essere stipulato dalle associazioni sindacali comparativamente più rappresentative sul piano nazionale. In mancanza di accordo, gli impianti e gli strumenti di cui al primo periodo possono essere installati previa autorizzazione della sede territoriale dell'Ispettorato nazionale del lavoro o, in alternativa, nel caso di imprese con unità produttive dislocate negli ambiti di competenza di più sedi territoriali, della sede centrale dell'Ispettorato nazionale del lavoro. I provvedimenti di cui al terzo periodo sono definitivi.*
- 2. La disposizione di cui al comma 1 non si applica agli strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa e agli strumenti di registrazione degli accessi e delle presenze.*
- 3. Le informazioni raccolte ai sensi dei commi 1 e 2 sono utilizzabili a tutti i fini connessi al rapporto di lavoro a condizione che sia data al lavoratore adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli e nel rispetto di quanto disposto dal decreto legislativo 30 giugno 2003, n. 196.”*

Pertanto, attraverso questo documento UTIU si prefigge i seguenti scopi.

Innanzitutto, quello d'individuare gli strumenti utilizzati dal lavoratore e le modalità con le quali la stessa effettua controlli per proteggere i beni e le informazioni aziendali e garantirne la sicurezza.

In secondo luogo, quello d'informare i suoi dipendenti e collaboratori.

Infine, quello di documentare tutte queste attività per garantire ed essere in grado di dimostrare all'occorrenza che i trattamenti in questione sono effettuati in conformità al Regolamento e alla legge sopracitati.

---

## DEFINIZIONI

Ai sensi del comma 1° dell'art. 4 del Regolamento UE 2016\679 sono date le seguenti definizioni:

<b>dato personale</b>	qualsiasi informazione riguardante una persona fisica, identificata o identificabile (interessato); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare a un identificativo come il nome, un numero d'identificazione, dati relativi all'ubicazione, un identificativo on line, o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;
<b>trattamento</b>	qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;
<b>limitazione di trattamento</b>	il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento;
<b>profilazione</b>	qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica;
<b>pseudonimizzazione</b>	il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile

<b>archivio</b>	qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico;
<b>titolare del trattamento</b>	la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;
<b>responsabile del trattamento</b>	la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;
<b>destinatario</b>	la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Tuttavia le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine non sono considerate destinatari;
<b>Consenso dell'interessato</b>	qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento;
<b>violazione dei dati personali</b>	la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati;
<b>dati relativi alla salute</b>	i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute;
<b>incaricati</b>	le persone fisiche autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile;

## 2 - INDIVIDUAZIONE DEGLI STRUMENTI DI LAVORO

### STRUMENTI UTILIZZATI DAL LAVORATORE

Nell'ambito dello svolgimento della prestazione lavorativa da parte del personale dipendente e dei collaboratori di UTIU, anche fuori dei locali aziendali, sono utilizzati i seguenti strumenti:

- a) i personal computer e le relative apparecchiature periferiche presenti all'interno dei locali di UTIU a prescindere dal fatto che siano connessi alla rete aziendale;
- b) la rete aziendale e tutte le sue componenti hardware e software che consentono le comunicazioni sia all'interno della rete locale, sia nelle reti geografiche (Internet);
- c) i dispositivi fisici e logici per assicurare la protezione della rete da accessi non autorizzati e da malfunzionamenti dipendenti da virus informatici;
- d) i dispositivi fisici e logici per assicurare i servizi di backup e restore del sistema informatico e dei relativi dati;
- e) i personal computer e gli altri dispositivi portatili (tablet, smartphone, ecc.) affidati da UTIU al lavoratore, con le relative applicazioni installate;
- f) i programmi operativi di base e i programmi applicativi necessari per l'attività produttiva, sia residenti sui server aziendali, sia quelli messi a disposizione con servizi di cloud computing;
- g) i siti web aziendali con le relative informazioni e i contenuti intellettuali;
- h) le chat, le video-chat, i sistemi di audio e video-conferenza, i forum attivati nella piattaforma di e-learning e nell'attività di formazione a distanza, con le relative informazioni e i contenuti intellettuali;
- i) l'account di posta elettronica individuale del lavoratore e quello condiviso con altri lavoratori attivato sul dominio aziendale, nonché il relativo servizio di comunicazione e di gestione e archiviazione dei messaggi;
- j) le credenziali di autenticazione individuali per l'accesso alla rete aziendale e/o ai programmi applicativi e/o ai servizi di cloud computing;
- k) il centralino telefonico e i suoi dispositivi individuali e il relativo servizio di comunicazione VOIP;
- l) gli archivi fisici e logici con i documenti in essi contenuti;
- m) il mobilio, gli arredi e il materiale di cancelleria.

A seconda delle mansioni o dei compiti affidati a ciascun lavoratore gli strumenti sopra elencati possono essere in tutto o in parte necessari per rendere la prestazione di lavoro.

In linea di massima, durante l'attività lavorativa, è ammesso l'uso degli strumenti di lavoro per fini personali per un periodo di tempo limitato, purché ciò sia possibile in concreto, non siano pregiudicate le funzionalità degli strumenti o dei beni aziendali, non si violino i diritti di altri soggetti e in ogni caso, ciò non contrasti con gli obblighi contrattuali verso il datore di lavoro.

## STRUMENTI DI REGISTRAZIONE DEGLI ACCESSI E DELLE PRESENZE

All'interno dei locali aziendali sono stati installati degli strumenti di registrazione degli accessi in entrata e in uscita del personale dipendente che raccolgono le timbrature mediante l'impiego manuale di un dispositivo (badge magnetico) assegnato univocamente a ciascun lavoratore.

Questi strumenti sono connessi alla rete aziendale e trasmettono i dati rilevati mediante un software applicativo (Speed presenze).

Il programma consente l'elaborazione delle informazioni (dati anagrafici e cronologia delle timbrature) al fine di misurare la durata della prestazione lavorativa per stabilire l'esatta quantificazione della retribuzione periodica, nonché al fine di gestire correttamente il rapporto di lavoro, relativamente alla presenza o all'assenza fisica del lavoratore nel luogo di lavoro, in funzione dei diritti e dei doveri contrattuali in capo a entrambe le parti.

L'uso scorretto dello strumento può implicare anche la violazione dei doveri di lealtà e correttezza nei confronti del datore di lavoro e comportare l'irrogazione di sanzioni disciplinari a carico del lavoratore.

Sempre per il rilevamento delle presenze e anche per la gestione a distanza dell'attività lavorativa relativa alla richiesta di permessi, ferie o assenze per malattia (Smart Working) è stato installato nei locali aziendali un sistema digitale basato sul software EcosAgile che attraverso l'applicativo eClock (*App*) installato sul dispositivo mobile (smartphone, tablet, ecc.) del lavoratore, è in grado di rilevare la sua presenza al momento della timbratura e di gestire telematicamente la comunicazione delle sue richieste dei permessi, ferie e assenze e delle relative approvazioni.

Sia l'installazione dell'applicativo, sia l'uso del sistema sono facoltativi per il lavoratore, che è inoltre libero di tornare in qualunque momento ad utilizzare il sistema di rilevamento tramite badge.

Il lavoratore si autentica al sistema tramite credenziali di accesso univoche (user id e password), al primo avvio l'*App* lo avvisa sul fatto che verrà utilizzata la geolocalizzazione e con una pop-up informativa chiederà al medesimo il consenso, inoltre avviserà attraverso una icona colorata l'attivazione temporanea della geolocalizzazione (verde=attiva, grigia=spenta), i dati della geolocalizzazione saranno memorizzati dall'*App* solo quando lo richiederà l'interessato attivando il bottone d'ingresso o uscita per ciascuna timbratura.

Le informazioni registrate (ora e data, dati anagrafici, coordinate geografiche, mappa visuale) potranno essere controllate dal lavoratore sia in tempo reale, sia differito, nessun'altra funzionalità dell'*App* utilizzerà la geolocalizzazione, né sarà trasmessa qualche altra informazione relativa alla geolocalizzazione, né infine sarà monitorata sistematicamente la presenza del lavoratore, né tracciata la sua posizione e/o gli spostamenti.

Il sistema web EcoAgile opera in "Cloud" e la trasmissione dei dati è protetta da crittografia e alle informazioni possono accedere solo gli operatori della Titolare espressamente autorizzati.

Anche in questo caso l'uso scorretto dello strumento può implicare la violazione dei doveri di lealtà e correttezza nei confronti del datore di lavoro e comportare l'irrogazione di sanzioni disciplinari a carico del lavoratore.



## 3 - MODALITÀ DI UTILIZZO DEGLI STRUMENTI DI LAVORO E DELLE ATTIVITÀ DI CONTROLLO PER ESIGENZE DI SICUREZZA E PROTEZIONE DEL PATRIMONIO AZIENDALE

---

### USO DEL PC E DEI DISPOSITIVI PORTATILI

Il Personal computer affidato a ciascun lavoratore nella postazione fissa situata all'interno dei locali aziendali, sia quello portatile, insieme agli dispositivi portatili (tablet, smartphone, ecc.) sono lo strumento di lavoro principale per rendere la prestazione lavorativa.

Per tale ragione devono essere utilizzati con la massima cura e prevalentemente per lo svolgimento dell'attività lavorativa.

È ammesso l'uso del Personal computer o del dispositivo portatile per fini personali per un periodo di tempo limitato, purché ciò sia possibile in concreto, non siano pregiudicate le sue funzionalità, non si violino i diritti di altri soggetti e in ogni caso, ciò non contrasti con gli obblighi contrattuali verso il datore di lavoro.

È possibile che gli strumenti siano configurati in modo da non consentire talune funzionalità, quali il collegamento di periferiche esterne o di memorie di massa allo scopo di evitare un potenziale conflitto tra gli apparati, l'estrazione di dati o la trasmissione di programmi informatici dannosi.

Vige il divieto assoluto di alterare, modificare, smontare, sottrarre o danneggiare, anche in modo involontario, il Personal computer o il dispositivo portatile affidato. In caso di violazione ciascun lavoratore potrà essere chiamato a rispondere delle sue responsabilità anche in sede disciplinare a seconda della gravità del suo comportamento e delle conseguenze causate all'azienda.

In caso di guasto o malfunzionamento, ovvero di furto del dispositivo portatile il lavoratore dovrà avvisare immediatamente il suo superiore gerarchico o il Responsabile dell'area IT.

Al termine della prestazione lavorativa o del rapporto di lavoro, il lavoratore è tenuto a restituire il dispositivo portatile affidatogli, curando di rimuovere o cancellare tutte le sue informazioni riservate o personali.

In caso contrario vi provvederà il personale dell'area IT immediatamente dopo la riconsegna.

---

### USO DEI PROGRAMMI APPLICATIVI

I programmi applicativi sono alla pari del PC lo strumento di lavoro principale per rendere la prestazione lavorativa.

Per tale ragione devono essere utilizzati con la massima cura e in modo esclusivo o, a seconda dei casi, prevalente per lo svolgimento dell'attività lavorativa.

È ammesso l'uso del programma applicativo per fini personali nei limiti delle possibilità di un suo utilizzo promiscuo e per un periodo di tempo limitato, purché ciò non pregiudichi le sue funzionalità, non si violino i diritti di altri soggetti e in ogni caso, ciò non contrasti con gli obblighi contrattuali verso il datore di lavoro.

L'accesso al sistema della rete aziendale, così come l'accesso ai programmi applicativi residenti o messi a disposizione tramite un servizio di cloud computing deve essere sempre configurato con una procedura di autenticazione individuale e univoca e sempre protetta da password. La password deve restare riservata e deve essere aggiornata periodicamente.

È fatto divieto di accedere al sistema o ai programmi applicativi attraverso le credenziali di autenticazione di un altro operatore, salvo che la condivisione delle credenziali sia imposta dalla particolare configurazione del programma o espressamente prevista dal Responsabile dell'area IT.

Laddove i criteri di configurazione delle password siano decisi dall'area IT aziendale, ciascun lavoratore dovrà rispettarne le policy preventivamente comunicate, mentre sarà un suo obbligo conoscere e rispettare i suddetti criteri nel caso siano decisi e resi noti dai produttori o dai fornitori esterni dei programmi applicativi attraverso i manuali operativi.

È possibile che il programma operativo di base o i singoli programmi applicativi siano configurati in modo da non consentire talune funzionalità, quali a titolo esemplificativo: il download di dati, l'installazione di programmi, la copia in locale, tutto ciò allo scopo di evitare un potenziale conflitto tra i programmi, l'alterazione del sistema, l'estrazione di dati o la trasmissione di programmi informatici dannosi.

Vige il divieto assoluto di alterare, modificare o danneggiare, anche in modo involontario, i programmi informatici utilizzati per rendere la prestazione lavorativa, inclusa la configurazione stabilita dagli amministratori di sistema. In caso di violazione ciascun lavoratore potrà essere chiamato a rispondere delle sue responsabilità anche in sede disciplinare a seconda della gravità del suo comportamento e delle conseguenze causate all'azienda.

In caso di guasto o malfunzionamento, ovvero di azione di programmi dannosi (virus) il lavoratore dovrà avvisare immediatamente il suo superiore gerarchico o il Responsabile dell'area IT.

Al termine della prestazione lavorativa il lavoratore è tenuto a effettuare, se necessario, il log-off del programma applicativo.

I programmi per la navigazione web e i servizi di posta elettronica hanno più di altri strumenti di lavoro una duplice valenza d'impiego.

Da una parte sono strumenti utili e talvolta necessari per rendere la prestazione lavorativa, dall'altra sono suscettibili di utilizzo personale quasi contemporaneo.

Di conseguenza è necessario dettagliarne l'uso in ambito lavorativo.

I programmi che consentono la navigazione nelle reti geografiche (Internet) possono essere utilizzati dal lavoratore per fini personali per un periodo di tempo limitato, purché ciò non causi dei pregiudizi al sistema informatico e ai beni aziendali, non siano violati i diritti di altri soggetti e in ogni caso, ciò non contrasti con gli obblighi contrattuali verso il datore di lavoro.

La navigazione web può esporre il sistema informatico e ai beni aziendali all'azione di programmi dannosi (virus), o di altre minacce informatiche (intrusioni e accessi abusivi), oppure può consentire l'accesso a contenuti informativi, immagini, suoni e video in violazione della legge o del diritto altrui.

Pertanto, l'uso dello strumento da parte del lavoratore, sia nell'ambito della prestazione lavorativa, sia durante il temporaneo uso personale, deve essere sempre improntato alla prudenza, prediligendo l'accesso a siti web noti in termini di affidabilità, sicurezza e rispetto della legalità.

Attualmente il sistema informatico aziendale è protetto da dispositivi antivirus e firewall, configurati dagli amministratori di sistema dell'area IT, che impediscono in modo relativo l'azione di programmi dannosi o di altre minacce informatiche.

È inoltre possibile che il programma di navigazione web e i dispositivi antivirus e firewall siano configurati dagli amministratori di sistema dell'area IT in modo da:

- selezionare i siti web considerati correlati o meno alla prestazione lavorativa;
- filtrare l'attività di navigazione impedendo l'accesso a determinati siti o l'esecuzione di certe attività come il download di file;
- tracciare in forma anonima e per periodi di tempo limitati il traffico web allo scopo di rilevare l'esistenza di una minaccia o l'azione di programmi dannosi.

Ciò non consente al lavoratore di eludere l'obbligo di adottare un comportamento prudente durante la navigazione e di astenersi dalla commissione di violazioni della legge o del diritto altrui. In caso di violazione di questi obblighi di protezione e collaborazione ciascun lavoratore potrà essere chiamato a rispondere delle sue responsabilità anche in sede disciplinare a seconda della gravità del suo comportamento e delle conseguenze causate all'azienda.

Il servizio di posta elettronica rappresenta lo strumento più delicato tra tutti quelli messi a disposizione del lavoratore, sia perché, alla pari del programma di navigazione web, espone il sistema informatico e ai beni aziendali all'azione di programmi dannosi (virus), o di altre minacce informatiche (intrusioni e accessi abusivi), sia perché consente un uso potenzialmente

più promiscuo rispetto agli altri. Infatti, l'indirizzo di posta elettronica individuale è suscettibile di essere impiegato anche per la corrispondenza personale.

Nell'ambito del dominio di posta aziendale è possibile creare account individuali o condivisi.

Laddove il servizio di posta elettronica è maggiormente utilizzato per rendere la prestazione lavorativa sono stati istituiti account di posta condivisi e quindi accessibili da più persone all'interno dell'azienda, con l'obiettivo principale di condividere i messaggi ricevuti e i relativi allegati, allo scopo di assicurare l'efficiente e continuo svolgimento dell'attività aziendale e provvedere alla loro conservazione e alla successiva consultazione, prescindendo dalla disponibilità del singolo lavoratore.

Nel caso invece di attribuzione di un account di posta individuale collegato al dominio aziendale il comportamento del lavoratore deve essere improntato alla prudenza, nonché alla massima correttezza e collaborazione nei confronti di UTIU al fine di consentire lo svolgimento dell'attività lavorativa.

Pertanto, è consentito l'uso personale dell'account di posta individuale del lavoratore a condizione che ciò non pregiudichi la sicurezza del sistema informatico e i beni aziendali, non violi i diritti di altri soggetti e in ogni caso, non contrasti con gli obblighi contrattuali verso il datore di lavoro.

Nel caso in cui l'account individuale è utilizzato nelle attività didattiche (Tutorato a distanza diacronico), l'uso dello strumento deve essere sempre improntato anche al rispetto dei ruoli e della dignità degli studenti.

Durante le assenze prolungate è prevista l'adozione di una risposta automatica o il reindirizzamento a un altro indirizzo di posta del dominio aziendale.

Al termine del rapporto di lavoro, il lavoratore è tenuto a cancellare o rimuovere i messaggi di posta personali e trasmettere al suo Responsabile gerarchico o ad altro soggetto indicato da UTIU quei messaggi il cui contenuto è rilevante per la prosecuzione dell'attività aziendale.

A tal fine il lavoratore viene invitato dal Responsabile dell'ufficio del personale a effettuare queste attività entro 5 giorni. In caso di violazione di questo obbligo di collaborazione il lavoratore potrà essere chiamato a rispondere delle sue responsabilità.

Scaduto questo termine il suo account individuale è cancellato insieme ai dati in esso contenuti.

---

## USO DEGLI STRUMENTI DI FORMAZIONE A DISTANZA

Le attività di formazione a distanza attivate nel cyberspazio didattico implicano l'uso di strumenti specifici per l'erogazione delle prestazioni di Tutorato a distanza sincronico.

Questi strumenti sono le chat, le video-chat, i sistemi di audio e video-conferenza, i forum attivati nella piattaforma di e-learning e nell'attività di formazione a distanza.

L'uso personale di questi strumenti da parte del lavoratore è consentito in misura limitatissima dato che essi interagiscono in tempo reale con una pluralità di studenti e possono interferire sulle attività didattiche e formative oltre a essere potenzialmente lesivo per la loro dignità.

Ne consegue che il loro uso deve essere sempre improntato alla massima prudenza, al rispetto dei ruoli e della dignità degli studenti. In caso di violazione di questi obblighi di collaborazione e protezione il lavoratore potrà essere chiamato a rispondere delle sue responsabilità anche in sede disciplinare a seconda della gravità del suo comportamento e delle conseguenze causate all'azienda.

Inoltre, l'uso di questi strumenti è soggetto a registrazione e archiviazione anche allo scopo di consentire agli studenti una fruizione successiva.

---

## USO DEGLI STRUMENTI DI LAVORO MANUALI

Il telefono, il materiale di cancelleria, il mobilio e gli arredi della postazione di lavoro sono gli strumenti tradizionali per rendere la prestazione lavorativa.

È ammesso l'uso di questi strumenti, in particolare il telefono e il materiale di cancelleria, per fini personali per un periodo di tempo limitato e in quantità molto limitata, purché ciò non arrechi un sensibile danno economico al datore di lavoro e non si violino i diritti di altri soggetti.

Il lavoratore deve utilizzare il mobilio, gli arredi e gli armadi adibiti ad archivio fisico con la massima cura, preservandoli da danni o pericoli. In caso di violazione di questo obbligo di protezione il lavoratore potrà essere chiamato a rispondere delle sue responsabilità anche in sede disciplinare a seconda della gravità del suo comportamento e delle conseguenze causate all'azienda.

data creazione del documento: 18/05/2018

data ultima revisione del documento: 01/12/2023