



# COMUNE DI MINERVINO DI LECCE

## Provincia di Lecce

### COPIA DI DELIBERAZIONE DELLA GIUNTA COMUNALE

Numero 76 del 16-05-2019

**Oggetto:** Regolamento UE 679/2016 - Approvazione Discipline per l'utilizzo degli strumenti informatici, della posta elettronica e di Internet

L'anno duemiladiciannove addì sedici del mese di maggio alle ore 13:30, in Minervino di Lecce nella sala delle adunanze del Palazzo Municipale, regolarmente convocata, si è riunita la Giunta Comunale per trattare gli argomenti posti all'ordine del giorno.

Presiede l' adunanza il Sig. Dott. Fausto De Giuseppe e sono rispettivamente presenti e assenti i seguenti Assessori:

<b>Dott. Fausto De Giuseppe</b>	<b>Sindaco</b>	<b>P</b>
<b>Assessore Urso Rossano</b>	<b>Vicesindaco</b>	<b>A</b>
<b>Corvaglia Sergio</b>	<b>Assessore</b>	<b>P</b>
<b>Carrisi Stefania</b>	<b>Assessore</b>	<b>A</b>
<b>DE MARCO FRANCESCA</b>	<b>Assessore</b>	<b>P</b>

ne risultano presenti n. 3 e assenti n. 2.

Partecipa il Segretario Marra dott. Fabio

Il Presidente, riconosciuta la validità del numero legale degli intervenuti per poter deliberare, dichiara aperta la seduta.

**PARERE:**Favorevole sulla proposta per la regolarità tecnica.

Minervino di Lecce, 13-05-19

Il Responsabile del Servizio  
f.to Marzo Alessandro

## LA GIUNTA COMUNALE

**RICHIAMATO** l'art. 42, c.2, lett. a), D.Lgs. 18 agosto 2000 n.267;

### **PREMESSO CHE:**

- il Parlamento europeo ed il Consiglio in data - 27.4.2016 hanno approvato il Regolamento UE 679/2016 (GDPR- *General Data Protection Regulation*) relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, che abroga la direttiva 95/46/CE e che mira a garantire una disciplina uniforme ed omogenea in tutto il territorio dell'Unione europea;
- il testo, pubblicato nella Gazzetta Ufficiale dell'Unione Europea (GUUE) il 4 maggio 2016, è diventato definitivamente applicabile in via diretta in tutti i Paesi UE a partire dal 25 maggio 2018, dopo un periodo di transizione di due anni, in quanto non richiede alcuna forma di legislazione applicativa o attuativa da parte degli stati membri;
- il Garante per la protezione dei dati personali ha emanato una Guida all'applicazione del Regolamento europeo in materia di protezione dei dati personali che intende offrire un panorama delle principali problematiche che i soggetti pubblici, oltre alle imprese, dovranno tenere presente in vista della piena applicazione del Regolamento;
- ai sensi dell'art.13 della Legge n.163/2017 il Governo è stato delegato ad adottare, entro sei mesi dalla sua entrata in vigore, uno o più decreti legislativi al fine di adeguare il quadro normativo nazionale alle disposizioni del Regolamento (UE) 2016/679 del 27 aprile 2016 di che trattasi;

### **RILEVATO CHE:**

- le norme introdotte dal Regolamento UE 2016/- 679 si traducono in obblighi organizzativi, documentali e tecnici che tutti i Titolari del trattamento dei dati personali devono, fin da subito, considerare e tenere presenti per consentire la piena e consapevole applicazione del nuovo quadro normativo in materia di privacy;
- appare necessario ed opportuno stabilire modalità organizzative, misure procedurali e regole di dettaglio, finalizzate anche ad omogeneizzare questioni interpretative, che permettano a questo Ente di poter agire con adeguata funzionalità ed efficacia nell'attuazione delle disposizioni introdotte dal nuovo Regolamento UE;

**Visto** il regolamento attuativo del Regolamento UE 2016/679 in materia di protezione dati personali, approvato con delibera di C.C. n.1 del 29/3/2019

### **Preso atto che:**

I servizi di rete, tra cui posta elettronica e Internet, rappresentano strumenti quotidiani indispensabili per l'esercizio dell'attività lavorativa e consentono l'immediatezza, la trasparenza e la trasversalità dell'informazione.

Poiché le informazioni di carattere personale trattate possono riguardare, oltre all'attività lavorativa, la sfera personale e la vita privata di lavoratori e di terzi, l'utilizzo delle risorse informatiche messe a disposizione del personale deve sempre ispirarsi ai principi di diligenza e correttezza, atteggiamenti richiesti nello svolgimento di ogni atto o comportamento posto in essere nell'ambito del rapporto di lavoro, in qualsiasi forma esso sia.

La protezione dei dati personali e delle informazioni nel loro complesso è condizione necessaria per garantire il rispetto dei requisiti di sicurezza che la normativa vigente impone a tutti i soggetti che, a vario titolo, effettuano il trattamento di dati personali.

Il datore di lavoro deve assicurare la funzionalità e il corretto impiego degli strumenti informatici da parte dei lavoratori.

**Tenuto conto che,**

al fine di adottare indirizzi trasparenti, capaci di comunicare con estrema chiarezza al lavoratore le corrette modalità di utilizzo degli strumenti informatici assegnatigli per lo svolgimento delle mansioni attribuite, definire con altrettanta chiarezza il diritto dell'Amministrazione a verificare l'uso corretto dei suddetti strumenti, individuare le modalità con cui l'Amministrazione esercita tale diritto di verifica e, soprattutto, evitare che comportamenti inconsapevoli possano innescare problemi o minacce alla sicurezza del sistema informatico e dei dati in esso contenuti e scambiati, è stato appositamente predisposto un disciplinare, che si allega;

**Visto** l' Art. 48. Competenze delle giunte del TUEL (D.lgs. 267/00)

**VISTO** il parere di regolarità tecnica espresso dal responsabile ai sensi dell'art. 49, Tuel;

Tanto premesso,

Con voti FAVOREVOLI/UNANIMI , espressi palesemente,

**DELIBERA**

1. Di approvare il Disciplinare per l'utilizzo degli strumenti informatici, della posta elettronica e di Internet che, allegato alla presente deliberazione, ne forma parte integrante e sostanziale;

2. Comunicare il presente disciplinare a tutti gli operatori/dipendenti dell'ente

**LA GIUNTA COMUNALE**

Con separata ed unanime votazione palese

**DELIBERA**

**DI DICHIARARE** la presente deliberazione immediatamente eseguibile ai sensi del 4 comma dell'art. 134 del citato D.Lgs. 267/2000.

Sottoscritto come per legge.

Il Presidente  
f.to Dott. Fausto De Giuseppe

Il Segretario  
f.to Dott. Marra dott. Fabio

---

---

La presente deliberazione è stata pubblicata all'Albo Pretorio di questo Comune in data odierna per rimanervi quindici giorni consecutivi.

Minervino di Lecce, li 20-05-2019

Il Responsabile alla pubblicazione  
f.to Marra dott. Fabio

Per Copia conforme all'originale

Minervino di Lecce, 20-05-2019

Il Segretario  
Dott. Marra dott. Fabio

---

---

SI ATTESTA

Che la presente Deliberazione è stata comunicata con lettera n. **4048** in data **20-05-2019** ai signori capigruppo consiliari così come prescritto dall'art. 125 del D. Lgs. 18.8.2000, n. 267;

La presente deliberazione diventa esecutiva per :

Dichiarazione di immediata eseguibilità (art. 134 c. 4°  
(S=si) T.U.E.L.. 267/2000).  
(N=no)

Decorrenza gg. 10 dalla pubblicazione ( art. 134 c. 3°  
T.U.E.L. n. 267/2000)

Minervino di Lecce, li 20-05-2019

Il SEGRETARIO COMUNALE  
F.to Dott. Marra dott. Fabio

# Disciplinare per l'uso degli strumenti informatici, della posta elettronica e di Internet

## Sommario

Sommario .....	1
1. Premessa .....	2
2. Titolarità degli strumenti e delle apparecchiature informatiche.....	2
3. Rispetto della proprietà intellettuale e delle licenze .....	2
4. Utilizzo dei dati e del software .....	3
5. Utilizzo della posta elettronica.....	3
6. Utilizzo dei servizi di rete e del collegamento a Internet.....	3
7. Monitoraggio e controlli .....	5

## **1. Premessa**

I servizi di rete, tra cui posta elettronica e Internet, sono rappresentati da strumenti quotidiani indispensabili per l'esercizio dell'attività lavorativa e consentono l'immediatezza, la trasparenza e la trasversalità dell'informazione.

Poiché le informazioni di carattere personale trattate possono riguardare, oltre all'attività lavorativa, la sfera personale e la vita privata di lavoratori e di terzi, l'utilizzo delle risorse informatiche messe a disposizione del personale deve sempre ispirarsi ai principi di diligenza e correttezza, atteggiamenti richiesti nello svolgimento di ogni atto o comportamento posto in essere nell'ambito del rapporto di lavoro, in qualsiasi forma esso sia.

La protezione dei dati personali e delle informazioni nel loro complesso è condizione necessaria per garantire il rispetto dei requisiti di sicurezza che la normativa vigente impone a tutti i soggetti che, a vario titolo, effettuano il trattamento di dati personali.

Il datore di lavoro deve assicurare la funzionalità e il corretto impiego degli strumenti informatici da parte dei lavoratori.

Il presente disciplinare, quindi, persegue le seguenti finalità:

- adottare indirizzi trasparenti, capaci di comunicare con estrema chiarezza al lavoratore le corrette modalità di utilizzo degli strumenti informatici assegnatigli per lo svolgimento delle mansioni attribuite;
- definire con altrettanta chiarezza il diritto dell'Amministrazione a verificare l'uso corretto dei suddetti strumenti;
- individuare le modalità con cui l'Amministrazione esercita tale diritto di verifica.

Il presente disciplinare è diretto anche ad evitare che comportamenti inconsapevoli possano innescare problemi o minacce alla sicurezza del sistema informatico e dei dati in esso contenuti e scambiati.

## **2. Titolarità degli strumenti e delle apparecchiature informatiche**

Il Comune di Minervino è proprietario degli strumenti e delle apparecchiature informatiche assegnati ai dipendenti o collaboratori. Tali strumenti sono affidati ai medesimi a condizione che vengano custoditi con cura, evitando manomissioni, danneggiamenti o utilizzi, anche da parte di altre persone, per scopi non consentiti.

Le risorse informatiche fornite dal Comune di Minervino devono essere utilizzate unicamente per perseguire gli scopi lavorativi. I dipendenti dell'Ente sono tenuti a rispettare la legge e le eventuali direttive di volta in volta emanate dall'Amministrazione.

## **3. Rispetto della proprietà intellettuale e delle licenze**

Tutto il personale è tenuto al rispetto delle leggi in materia di tutela della proprietà intellettuale e non può, sulle apparecchiature fornite, installare hardware o software né duplicare o utilizzare software che non sia stato preinstallato, installato o comunque fornito dall'Amministrazione.

#### **4. Utilizzo dei dati e del software**

I dati e le informazioni detenute su apparecchiature o altri supporti sono utilizzati dal personale ai soli fini lavorativi. Nessun dato può essere trattato o memorizzato su dispositivi di qualsiasi tipologia, non finalizzati all'attività lavorativa.

#### **5. Utilizzo della posta elettronica**

Il servizio di posta elettronica erogato dal sistema informatico è ad uso del Comune di Minervino .

L'assegnazione delle caselle di posta elettronica ai dipendenti è finalizzata all'utilizzo di tale mezzo di comunicazione per lo svolgimento dell'attività lavorativa. Ogni comunicazione via posta elettronica con soggetti esterni od interni all'Amministrazione deve avvenire mediante l'utilizzo del sistema di posta elettronica dell'Ente, per garantire i necessari livelli di sicurezza e riservatezza.

Non sono consentiti gli utilizzi finalizzati a divulgare contenuti illeciti o altrimenti inaccettabili, oppure finalizzati a violare i diritti legali altrui. Al dipendente è vietato intercettare, alterare, impedire o interrompere comunicazioni di altri utenti ed installare apparecchiature e programmi idonei a tale scopo.

#### **6. Utilizzo dei servizi di rete e del collegamento a Internet**

Il collegamento a Internet ed i servizi di rete messi a disposizione dall'Ente sono finalizzati all'utilizzo per lo svolgimento dell'attività lavorativa. Sulla rete aziendale non è consentito utilizzare dispositivi e software di rete che non siano stati preventivamente autorizzati dall'Amministrazione.

- Il personal computer, e gli altri eventuali strumenti elettronici, sono affidati all'incaricato, con ogni conseguente obbligo di custodia e di utilizzo appropriato. L'incaricato è tenuto ad informare immediatamente l'Amministrazione nell'ipotesi di furto, danneggiamento o malfunzionamento anche parziale degli stessi, del sistema o del software installato.
- L'incaricato deve utilizzare gli strumenti elettronici con la massima attenzione e diligenza, essendo beni rilevanti anche ai fini della sicurezza. Gli strumenti sono configurati in modo da garantire il rispetto delle regole descritte nel presente disciplinare; tale configurazione non deve essere mutata.
- L'accesso al sistema operativo del personal computer, o degli altri strumenti elettronici, è condizionato al corretto inserimento delle credenziali di autenticazione (nome utente e password).
- L'incaricato è tenuto a modificare la propria password nel rispetto dei criteri previsti dalle istruzioni/procedure. In ogni caso, l'incaricato è tenuto a modificare la propria password, comunque nel rispetto dei criteri suddetti, allorché ritenga che altri possa in qualsiasi modo esserne venuto a conoscenza o che possa comunque esserne venuta meno la segretezza.

- Non è consentita la modifica delle impostazioni di sicurezza e di riservatezza del sistema operativo, del software di posta elettronica, e di ogni altro software installato sui personal computer, sui dispositivi elettronici o sul sistema.
- Non è consentito caricare o comunque detenere nei personal computer o nei dispositivi materiale informatico, dati ed informazioni personali o comunque di contenuto non attinente alla mansione ricoperta.
- È in ogni caso tassativamente vietato caricare o detenere materiale informatico il cui contenuto sia contrario a norme di legge e/o comunque per finalità ludiche o di svago.

L'incaricato deve:

- spegnere l'elaboratore, gli altri strumenti elettronici ed eventuali periferiche (stampanti, scanner, ecc.) prima di lasciare l'ufficio al termine dell'attività lavorativa o in caso di allontanamenti protratti dal posto di lavoro e deve comunque adottare le altre cautele previste dalle procedure/istruzioni, anche in caso di brevi allontanamenti;
- far eseguire le operazioni di manutenzione/riparazione degli strumenti solo da parte del personale autorizzato dall'Amministrazione;
- evitare qualsiasi uso di strumenti elettronici personali (pc, periferiche, dispositivi di memorizzazione, ecc.) sul luogo di lavoro o per usi lavorativi;
- non alterare o disattivare le altre misure di sicurezza adottate dal Comune di Minervino ed anzi effettuare quanto di competenza per garantirne il funzionamento, segnalando tempestivamente ogni anomalia o disfunzione;
- non impostare password o analoghe protezioni ai singoli archivi informatici (dischi, cartelle o files), al di fuori di quelle previste dalle procedure interne, dalla configurazione del sistema, o da specifiche istruzioni scritte.
- Tutta la gestione degli strumenti elettronici, incluse le modifiche alla configurazione dei sistemi desktop e portatili, può essere effettuata unicamente dal Comune di Minervino o da soggetti espressamente e formalmente autorizzati. Gli incaricati non sono autorizzati a modificare il sistema neppure se si tratta della postazione di lavoro assegnata. A titolo esemplificativo ma non esaustivo, si enunciano attività che sono considerate modifiche del sistema:
  - modificare i collegamenti di rete esistenti;
  - usare dispositivi removibili per alterare la procedura di avvio del dispositivo ·
  - aprire la struttura esterna (case) dell'elaboratore e procedere alla modifica (eliminazione o aggiunta) di componenti dello stesso;
  - alterare la configurazione del pc ricevuta in assegnazione.
- Le cartelle utenti presenti nei server sono aree di condivisione di informazioni strettamente professionali e non possono in alcun modo essere utilizzate per scopi diversi. Pertanto qualunque file che non sia legato all'attività lavorativa non può essere dislocato, nemmeno per brevi periodi, in queste unità. Su queste unità vengono svolte regolari attività di amministrazione e back-up da parte del personale incaricato. Si ricorda che tutti i dischi o altre unità di memorizzazione locali non



sono soggette a salvataggio dei dati ivi contenuti è pertanto a carico del singolo incaricato.

## **7. Monitoraggio e controlli**

A garanzia della sicurezza dei sistemi informativi e dei servizi di rete, è nella facoltà dell'Ente effettuare controlli preliminari su dati aggregati, riferiti all'intera struttura lavorativa o a sue aree, nonché predisporre controlli a campione, in forma anonima, sugli accessi ad Internet e sulla navigazione web. È sempre fatta salva l'ipotesi dell'attivazione di controlli, anche individualizzati, che trovino giustificazione nella necessità di corrispondere ad eventuali richieste di organi di polizia su segnalazione dell'autorità giudiziaria, nel verificarsi di un evento dannoso o una situazione di pericolo che richieda un immediato intervento o nella presenza di sospetti relativamente all'esistenza di condotte improprie nell'uso delle apparecchiature (cd. controlli difensivi).