

**ISTITUTO AUTONOMO PER LE CASE POPOLARI**  
***DELLA PROVINCIA DI FOGGIA***

**REGOLAMENTO INTERNO PER L'UTILIZZO DEI SISTEMI INFORMATICI  
E TELEFONICI**

**DELIBERA DEL COMMISSARIO STRAORDINARIO N. 230 DEL 18.11.2010**

**ISTITUTO AUTONOMO PER LE CASE POPOLARI**  
***DELLA PROVINCIA DI FOGGIA***

Indice

Premessa

Art. 1 Campo di applicazione del regolamento

Art. 2 Utilizzo del Personal Computer

Art. 3 Gestione ed assegnazione delle credenziali di autenticazione

Art. 4 Utilizzo della rete dell'Istituto

Art. 5 Utilizzo e conservazione dei supporti rimovibili

Art. 6 Utilizzo di PC portatili

Art. 7 Uso della posta elettronica

Art. 8 Navigazione in Internet

Art. 9 Protezione antivirus

Art. 10 Utilizzo dei software gestionali

Art. 11 Utilizzo dei telefoni, fax e fotocopiatrici aziendali

Art. 12 Osservanza delle disposizioni in materia di Privacy

Art. 13 Sistemi di controlli gradualità

Art. 14 Sanzioni

Art. 15 Entrata in vigore del regolamento e pubblicità

# **ISTITUTO AUTONOMO PER LE CASE POPOLARI**

## ***DELLA PROVINCIA DI FOGGIA***

### **Premessa**

La progressiva diffusione delle nuove tecnologie informatiche e, in particolare, il libero accesso alla rete internet dai personal computer, espone l'Istituto e i dipendenti a rischi di natura patrimoniale, oltre alle responsabilità penali conseguenti alla violazione di specifiche disposizioni di legge (legge 22 aprile 1941 n. 633 sul diritto d'autore e legge sulla privacy Dlgs n. 196/2003, fra tutte), creando evidenti problemi alla sicurezza ed all'immagine dell'Istituto stesso.

Premesso quindi che l'utilizzo delle risorse informatiche e telematiche deve sempre ispirarsi al principio della diligenza e correttezza nell'ambito del rapporto di lavoro, l'Istituto con il presente regolamento interno intende evitare che comportamenti inconsapevoli possano innescare problemi o minacce alla sicurezza nel trattamento dei dati.

Le prescrizioni di seguito previste si aggiungono ed integrano le specifiche istruzioni già fornite a tutti gli incaricati in attuazione del decreto legislativo 30 giugno 2003 n. 196 e ss.mm.ii., e del disciplinare tecnico (Allegato B al citato decreto legislativo) contenente le misure minime di sicurezza, nonché integrano le informazioni già fornite agli interessati in ordine alle ragioni e alle modalità dei possibili controlli o alle conseguenze di tipo disciplinare in caso di violazione delle stesse.

# **ISTITUTO AUTONOMO PER LE CASE POPOLARI**

## ***DELLA PROVINCIA DI FOGGIA***

### **Art. 1**

#### **Campo di applicazione del regolamento**

1. Il regolamento si applica a tutti i dipendenti dell'Istituto.

### **Art. 2**

#### **Utilizzo del personal computer**

1. Il personal computer affidato al dipendente è uno strumento di lavoro. Ogni utilizzo non inerente all'attività lavorativa è vietato perché può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza. Il personal computer deve essere custodito con cura evitando ogni possibile forma di danneggiamento.

2. Il personal computer dato in affidamento all'utente permette l'accesso alla rete LAN dell'ente solo attraverso specifiche credenziali di autenticazione come meglio descritto al successivo articolo 3.

3. L'Istituto rende noto che il personale incaricato che opera presso il CED è autorizzato a compiere interventi nel sistema informatico dell'Istituto diretti a garantire la sicurezza e la salvaguardia del sistema stesso, nonché per ulteriori motivi tecnici e/o manutentivi (ad es. aggiornamento/sostituzione/implementazione di programmi, manutenzione hardware etc.).

Detti interventi, in considerazione dei divieti di cui ai successivi articoli 7, comma 2 e 8, comma 1, possono anche comportare l'accesso in qualunque momento, ai dati trattati da ciascuno, ivi compresi gli archivi di posta elettronica, nonché alla verifica sui siti internet acceduti dagli utenti abilitati alla navigazione esterna. La stessa facoltà, sempre ai fini della sicurezza del sistema e per garantire la normale operatività dell'Istituto, si applica anche in caso di assenza prolungata od impedimento dell'utente.

4. Il personale del CED ha la facoltà di collegarsi e visualizzare in remoto il desktop delle singole postazioni PC al fine di garantire l'assistenza tecnica e la normale attività operativa nonché la massima sicurezza contro virus, spyware, malware, etc. L'intervento è effettuato esclusivamente su chiamata dell'utente o, in caso di oggettiva necessità, a seguito della rilevazione tecnica di problemi nel sistema informatico e telematico. In quest'ultimo caso, e sempre che non si pregiudichi la necessaria tempestività ed efficacia dell'intervento, è data comunicazione della necessità dell'intervento stesso.

# **ISTITUTO AUTONOMO PER LE CASE POPOLARI**

## ***DELLA PROVINCIA DI FOGGIA***

5. Non è consentito l'uso di programmi diversi da quelli ufficialmente installati dal personale del CED per conto dell'Istituto né viene consentito agli utenti di installare autonomamente programmi provenienti dall'esterno, sussistendo il grave pericolo di introdurre virus informatici e/o di alterare la funzionalità delle applicazioni software esistenti ed inoltre si configura come violazione della normativa a tutela dei diritti d'autore sul software, che impone la presenza nel sistema di software regolarmente licenziato, o comunque libero e quindi non protetto dal diritto d'autore.

Tali inosservanze sono sanzionate anche penalmente a carico degli autori oltre ad esporre lo stesso IACP a gravi responsabilità civili per le quali si rivarrà sugli stessi.

6. Salvo preventiva espressa autorizzazione del personale del CED, non è consentito all'utente modificare le caratteristiche impostate sul proprio PC né procedere ad installare dispositivi di memorizzazione, comunicazione o altro (come ad esempio masterizzatori, modem, etc.).

7. Ogni utente deve prestare la massima attenzione ai supporti di origine esterna, avvertendo immediatamente il personale del CED nel caso in cui siano rilevati virus ed adottando quanto previsto dal successivo articolo 9 relativo alle procedure di protezione antivirus.

8. Il personal computer deve essere spento ogni sera prima di lasciare gli uffici o in caso di assenze prolungate dall'ufficio o in caso di suo inutilizzo. In ogni caso, lasciare un elaboratore incustodito connesso alla rete può essere causa di utilizzo da parte di terzi senza che vi sia la possibilità di provarne in seguito l'indebito uso.

### **Art. 3**

#### **Gestione ed assegnazione delle credenziali di autenticazione per l'accesso alla rete**

1. Le credenziali di autenticazione per l'accesso alla rete sono assegnate dal personale del CED, previa formale richiesta del Dirigente o del Responsabile della unità organizzativa nell'ambito della quale è inserito e va ad operare il nuovo utente.

2. Le credenziali di autenticazione consistono in un codice per l'identificazione dell'utente (user id), assegnato dal CED, associato ad una parola chiave (password) riservata che deve venir custodita dall'incaricato con la massima diligenza e non divulgata. Non è consentita l'attivazione della password di accensione (bios), senza preventiva autorizzazione da parte del CED.

# **ISTITUTO AUTONOMO PER LE CASE POPOLARI**

## **DELLA PROVINCIA DI FOGGIA**

3. Le password devono essere lunghe almeno 8 caratteri, (salvo impedimenti tecnici delle applicazioni, o aggiornamenti normativi più stringenti), formate da lettere (maiuscole e/o minuscole), numeri e caratteri speciali quali &, %, ^, #, \$, ricordando che lettere maiuscole e minuscole hanno significati diversi per i sistemi, evitando ovviamente contenuti di senso logico immediato che sono facilmente individuabili (per es. nomi/date di nascita e simili).

4. È necessario procedere alla modifica della parola chiave a cura dell'utente, incaricato del trattamento, al primo utilizzo e, successivamente, almeno ogni tre mesi (ogni mese nel caso invece di trattamento di dati sensibili attraverso l'ausilio di strumenti elettronici).

### **Art. 4**

#### **Utilizzo della rete dell'Istituto**

1. Per l'accesso alla rete LAN dell'Istituto ciascun utente deve essere in possesso della specifica credenziale di autenticazione.

2. È assolutamente proibito entrare nella rete e nei programmi con un codice d'identificazione utente diverso da quello assegnato. Le password d'ingresso alla rete ed ai programmi sono segrete e vanno comunicate e gestite secondo le procedure impartite.

3. Le cartelle utenti (Documenti) presenti sulle unità Server di rete 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 controllo, amministrazione e backup da parte del personale CED. Tutti i dischi o altre unità di memorizzazione locali (es. disco C: interno PC) non sono soggette a salvataggio da parte del personale del CED. La responsabilità dei dati ivi contenuti è a carico del singolo utente, pertanto gli utenti devono utilizzare le cartelle personali create sui Server il cui accesso in scrittura e lettura è concesso solo all'utente e agli operatori di backup. Oltre alle cartelle personali, sono a disposizione delle aree condivise, a livello di settore ed altre a livello di unità organizzativa, in cui possono accedere in lettura e scrittura tutti gli utenti appartenenti rispettivamente allo stesso settore o unità organizzativa.

4. Il personale del CED può in qualunque momento procedere alla rimozione di ogni file o applicazione che ritiene essere pericolosi per la sicurezza sia sui PC degli incaricati sia sulle altre unità di rete.

# **ISTITUTO AUTONOMO PER LE CASE POPOLARI**

## ***DELLA PROVINCIA DI FOGGIA***

5. Risulta opportuno che, con regolare periodicità (almeno ogni tre mesi), ciascun utente provveda alla pulizia degli archivi, con cancellazione dei file obsoleti o inutili. Particolare attenzione deve essere prestata alla duplicazione dei dati, essendo infatti necessario evitare un'archiviazione ridondante.

6. Nel caso di cessazione del servizio e/o trasferimento di un dipendente, il Dirigente o il Responsabile dell'u.o. è tenuto ad impartire idonee istruzioni affinché i documenti di interesse per l'intero ufficio siano trasferiti in opportune aree accessibili dai colleghi, al fine di garantire la continuità del servizio ed il rispetto della privacy.

7. Rimane assolutamente vietato e sottoposto a sanzione, la pulizia del proprio computer in caso di cessazione del servizio e/o trasferimento, costituendo i file archiviati documentazione amministrativa di proprietà dell'Istituto.

### **Art. 5**

#### **Utilizzo e conservazione dei supporti rimovibili**

1. Tutti i supporti magnetici rimovibili (dischetti, CD e DVD riscrivibili, supporti USB, ecc.), contenenti dati sensibili nonché informazioni costituenti patrimonio informativo dell'Iacp di Foggia, devono essere trattati con particolare cautela onde evitare che il loro contenuto possa essere trafugato o alterato o diffuso impropriamente e/o distrutto o, successivamente alla cancellazione, recuperato.

2. Al fine di assicurare la distruzione e/o inutilizzabilità di supporti magnetici rimovibili contenenti dati sensibili, ciascun utente deve contattare il personale del CED e seguire le istruzioni da questo impartite.

3. In ogni caso, i supporti magnetici contenenti dati sensibili devono essere adeguatamente custoditi in armadi chiusi, a cura degli utenti.

4. E' vietato l'utilizzo di supporti rimovibili personali.

5. L'utente è responsabile della custodia dei supporti e dei dati dell'Istituto in essi contenuti.

# **ISTITUTO AUTONOMO PER LE CASE POPOLARI**

## **DELLA PROVINCIA DI FOGGIA**

### **Art. 6** **Utilizzo di PC portatili**

1. L'utente è responsabile del PC portatile assegnatogli dall'Istituto e deve custodirlo con diligenza sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro.
2. Ai PC portatili si applicano le regole di utilizzo previste dal presente regolamento, con particolare attenzione alla rimozione di eventuali file elaborati prima della riconsegna.
3. I PC portatili utilizzati all'esterno, in caso di allontanamento, devono essere custoditi con diligenza, adottando tutti i provvedimenti che le circostanze rendono necessari per evitare danni o sottrazioni.
4. Eventuali configurazioni di tipo accesso remoto, dirette verso la rete aziendale o attraverso internet, devono essere autorizzate esclusivamente dal Dirigente e configurate a cura del personale del CED.  
E' vietato utilizzare le suddette connessioni all'interno della sede dell'Istituto se contemporaneamente connessi alla rete LAN.

### **Art. 7** **Uso della posta elettronica**

1. La casella di posta elettronica assegnata all'utente è uno strumento di lavoro. Gli utenti assegnatari delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse.
2. È fatto divieto di utilizzare le caselle di posta elettronica per motivi diversi da quelli strettamente legati all'attività lavorativa.  
L'utente non può utilizzare la posta elettronica per:
  - a) l'invio e/o il ricevimento di allegati contenenti filmati o brani musicali (es.: mp3) non legati all'attività lavorativa;
  - b) l'invio e/o il ricevimento di messaggi personali o per la partecipazione a dibattiti, aste on line, concorsi, forum o mailing-list;
  - c) la partecipazione a catene telematiche (o di Sant'Antonio). Se si dovessero peraltro ricevere messaggi di tale tipo, si deve comunicarlo immediatamente al personale del CED. Non si deve in alcun caso procedere all'apertura degli allegati a tali messaggi.

**ISTITUTO AUTONOMO PER LE CASE POPOLARI**  
**DELLA PROVINCIA DI FOGGIA**

3. La casella di posta deve essere mantenuta in ordine, cancellando documenti inutili e soprattutto allegati ingombranti.
4. Ogni comunicazione inviata o ricevuta che abbia contenuti rilevanti o contenga impegni contrattuali o precontrattuali per l'Istituto ovvero contenga documenti da considerarsi riservati in quanto contraddistinti dalla dicitura "strettamente riservati" o da analoga dicitura, deve essere visionata od autorizzata dal Dirigente o dal Responsabile dell'u.o.
5. È possibile utilizzare la ricevuta di ritorno per avere la conferma dell'avvenuta lettura del messaggio da parte del destinatario.
6. È obbligatorio porre la massima attenzione nell'aprire i file attachments di posta elettronica prima del loro utilizzo (non eseguire download di file eseguibili o documenti da siti Web o Ftp non conosciuti).
7. Al fine di garantire la funzionalità del servizio di posta elettronica dell'Istituto, nel rispetto del principio di necessità e di proporzionalità, in caso di assenze programmate e/o in caso di prolungata assenza (ad es. per ferie o malattie o attività di lavoro fuori sede dell'assegnatario della casella) deve essere assegnata a cura del Dirigente ad altro dipendente la gestione della medesima casella di posta.
8. E' comunque consentito al superiore gerarchico dell'utente o, comunque, sentito l'utente, a persona individuata dall'Istituto, accedere alla casella di posta elettronica dell'utente per ogni ipotesi in cui si renda necessario (ad es.: funzionalità di cui all'articolo 7, comma 7).
9. Il personale del CED, nell'impossibilità di procedere come sopra indicato e nella necessità di non pregiudicare la necessaria tempestività ed efficacia dell'intervento, può accedere alla casella di posta elettronica per le finalità di tipo tecnico o manutentive indicate all'articolo 2, comma 3.
- 10 Al fine di ribadire agli interlocutori la natura esclusivamente legata all'attività istituzionale della casella di posta elettronica, i messaggi devono contenere un avvertimento standardizzato nel quale sia dichiarata la natura non personale dei messaggi stessi precisando che il personale debitamente incaricato dall'Istituto può accedere al contenuto del messaggio inviato alla stessa casella secondo le regole fissate dall'Istituto stesso.

# **ISTITUTO AUTONOMO PER LE CASE POPOLARI**

## **DELLA PROVINCIA DI FOGGIA**

### **Art. 8**

#### **Navigazione in internet**

1. Il PC assegnato al singolo utente ed abilitato alla navigazione in internet costituisce uno strumento aziendale utilizzabile esclusivamente per lo svolgimento della propria attività lavorativa. È quindi assolutamente proibita la navigazione in internet per motivi diversi da quelli strettamente legati all'attività lavorativa.

2. In questo senso, a titolo puramente esemplificativo, l'utente non può utilizzare internet per:

- a) l'upload o il download di software gratuiti (freeware) e shareware, nonché l'utilizzo di documenti provenienti da siti web, se non strettamente attinenti all'attività lavorativa (filmati e musica) e previa verifica dell'attendibilità dei siti in questione (nel caso di dubbio, deve venir a tal fine contattato il personale del CED);
- b) l'effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti on-line e simili, fatti salvi i casi direttamente autorizzati dall'Istituto e comunque nel rispetto delle normali procedure di acquisto;
- c) ogni forma di registrazione a siti i cui contenuti non siano strettamente legati all'attività lavorativa;
- d) la partecipazione a forum non professionali, l'utilizzo di chat line (esclusi gli strumenti autorizzati), di bacheche elettroniche e le registrazioni in guestbooks anche utilizzando pseudonimi (o nicknames) se non espressamente autorizzati dal Responsabile competente;
- e) l'accesso, tramite internet, a caselle webmail di posta elettronica personale.

3. Al fine di evitare la navigazione in siti non pertinenti all'attività lavorativa, l'Istituto rende peraltro nota l'adozione di un sistema definito proxy che consente tramite alcune applicazioni software determinati blocchi o filtri automatici che prevengano determinate operazioni quali l'upload o l'accesso a determinati siti inseriti in una black list o la consultazione di video in streaming ecc.

4. Gli eventuali controlli, compiuti dal personale incaricato del CED ai sensi del precedente articolo 2, comma 3, possono avvenire mediante un sistema di controllo dei contenuti (proxy server) o mediante "file di log" della navigazione svolta. Il controllo sui file di log viene effettuato dietro richiesta del Dirigente dell'utente ed i file stessi vengono conservati non oltre 7 giorni naturali, ossia il tempo indispensabile per il corretto perseguimento delle finalità organizzative e di sicurezza dell'Ente.

# **ISTITUTO AUTONOMO PER LE CASE POPOLARI**

## ***DELLA PROVINCIA DI FOGGIA***

5. Qualora il file di log venga utilizzato come prova in caso di provvedimento disciplinare, è compito del personale del CED, dietro autorizzazione del Dirigente competente, estrarre copia, memorizzarla su un supporto non riscrivibile e consegnarla allo stesso che provvede alla conservazione del supporto.

### **Art. 9**

#### **Protezione antivirus**

1. Il sistema informatico dell'Istituto è protetto da software antivirus aggiornato quotidianamente. Ogni utente deve comunque tenere comportamenti tali da ridurre il rischio di attacco al sistema informatico mediante virus o mediante ogni altro software aggressivo.
2. Nel caso il software antivirus rilevi la presenza di un virus, l'utente deve immediatamente sospendere ogni elaborazione in corso senza spegnere il computer nonché segnalare prontamente l'accaduto al personale del CED.
3. Ogni dispositivo magnetico di provenienza esterna all'Istituto deve essere verificato mediante il programma antivirus prima del suo utilizzo e, nel caso venga rilevato un virus, non può essere utilizzato fin tanto che il virus non è rimosso.

### **Art. 10**

#### **Utilizzo dei software gestionali**

1. Il sistema informatico dell'Istituto è dotato di software gestionali per agevolare ed ottimizzare le attività svolte da ogni dipendente. Tutto il software è regolarmente licenziato e supportato dalla ditta fornitrice.
2. A fronte dell'esigenza di mantenere banche dati aggiornate, coerenti e consistenti, durante le operazioni quotidiane di gestione viene eseguita una tracciatura delle sole operazioni che comportino una modifica ai dati. I log sono conservati per un tempo adeguato in relazione alle finalità specifiche e alle tecnologie impiegate.
3. Al fine di verificare la correttezza, la diligenza ed eventualmente l'accertamento di abusi collegati all'utilizzo dei sistemi informatici, possono essere attivati sistemi di tracciatura delle operazioni di consultazione delle informazioni. Il Responsabile del trattamento dati, prima dell'attivazione dà opportuna comunicazione ai dipendenti interessati.

# **ISTITUTO AUTONOMO PER LE CASE POPOLARI**

## **DELLA PROVINCIA DI FOGGIA**

### **Art. 11**

#### **Utilizzo dei telefoni, fax e fotocopiatrici dell'Istituto**

1. Il telefono e il fax dell'Istituto sono strumenti di lavoro. Ne viene concesso l'uso esclusivamente per lo svolgimento dell'attività lavorativa, non essendo quindi consentite comunicazioni a carattere personale o comunque non strettamente inerenti l'attività lavorativa stessa. La ricezione o l'effettuazione di telefonate e/o fax personali è consentito solo nel caso di comprovata necessità ed urgenza.
2. Qualora venisse assegnato un cellulare aziendale all'utente, quest'ultimo rimane responsabile del suo utilizzo e della sua custodia. Al cellulare aziendale si applicano le medesime regole sopra previste per l'utilizzo del telefono aziendale. L'eventuale uso promiscuo (anche per fini personali) del telefono cellulare aziendale è possibile soltanto in presenza di preventiva autorizzazione scritta e in conformità delle istruzioni al riguardo impartite dal personale della Segreteria Generale.
3. È vietato l'utilizzo delle fotocopiatrici aziendali per fini personali.

### **Art. 12**

#### **Osservanza delle disposizioni in materia di privacy**

1. È obbligatorio attenersi alle disposizioni in materia di privacy e di misure minime di sicurezza, come indicato dai Responsabili in materia di trattamento dei dati ai sensi del disciplinare tecnico allegato al decreto legislativo 30 giugno 2003, n.196.

### **Art. 13**

#### **Sistemi di controlli gradualali**

1. In caso di anomalie dei sistemi rilevate dal personale incaricato del CED, sono effettuati controlli che si concludono con avvisi, diretti ai dipendenti dell'area o del settore in cui è stata rilevata l'anomalia, nei quali si evidenzia l'utilizzo irregolare degli strumenti aziendali e si invitano gli interessati ad attenersi scrupolosamente ai compiti assegnati e alle istruzioni impartite. Controlli individuali possono essere autorizzati dal Dirigente competente in special modo dopo ripetute anomalie, delle quali deve essere tempestivamente informato da parte del personale del CED.
2. In nessun caso sono compiuti controlli prolungati, costanti o indiscriminati.

**ISTITUTO AUTONOMO PER LE CASE POPOLARI**  
***DELLA PROVINCIA DI FOGGIA***

Art. 14  
Sanzioni

1. È fatto obbligo a tutti gli utenti di osservare le disposizioni riportate nel presente regolamento. Il mancato rispetto o la violazione delle stesse è perseguibile nei confronti del personale dipendente con provvedimenti disciplinari e risarcitori previsti dal vigente Contratto collettivo nazionale di lavoro, nonché con le azioni civili e penali previste dalle vigenti norme.

Art. 15  
Entrata in vigore del regolamento e pubblicità

1. Il regolamento entra in vigore a seguito approvazione con delibera del Commissario Straordinario dell'Istituto.  
Con l'entrata in vigore del presente regolamento tutte le disposizioni in precedenza adottate in materia, in qualsiasi forma comunicate, devono intendersi abrogate e sostituite dalle presenti.
2. Copia del regolamento è pubblicato all'albo e sul sito dell'Istituto ed è consegnato a ciascun dipendente.