
# Northern Ireland Community Relations Council

# Information Security Policy

**May 2018**

## Document Control

The Current status of the document is issued Final.

| Version No. | Approval by | Approval date | Issue date |
|---|---|---|---|
| | | | |
| | | | |
| | | | |

# Information Security Policy

## 1. Introduction

This information security policy is a key component of the Community Relations Council's overall information security management framework and should be considered alongside other documentation including, Data Protection Policy, External Device Policy, Records Management and Document Retention Policy etc.

**Background to the Community Relations Council**

### 1.1 Community Relations Council

*Promoting a peaceful and fair society based on reconciliation and mutual trust*

The Community Relations Council (CRC) was established as an independent body in 1990 to lead and support change in Northern Ireland towards reconciliation, tolerance and mutual trust. CRC is the core strategic institution for inter-community and inter-cultural work at a regional level. By promoting better practice through constructive and relevant dialogue between different groups and sectors in society, the CRC is the lead advocate body on the achievement and maintenance of good community relations. CRC is funded by TEO and the organisation assists in the implementation of The Executive Office's Good Relations Strategy – Together: Building a United Community.

## 2. Objectives, Aim and Scope

### 2.1. Objectives

The objectives of the Community Relations Council's Information Security Policy are to preserve:

- **Confidentiality** - Access to Data shall be confined to those with appropriate authority.
- **Integrity** – Information shall be complete and accurate. All systems, assets and networks shall operate correctly, according to specification.
- **Availability** - Information shall be available and delivered to the right person, at the time when it is needed.

### 2.2. Policy aim

The aim of this policy is to establish and maintain the security and confidentiality of information, information systems, applications and networks owned or held by CRC or any third parties responsible for providing networks or software by:

- Ensuring that all members of staff are aware of and fully comply with the relevant legislation as described in this and other policies by providing training and clear policies for staff to follow.
- Describing the principals of security and explaining how they shall be implemented in the organisation.
- Introducing a consistent approach to security, ensuring that all members of staff fully understand their own responsibilities.
- Creating and maintaining within the organisation a level of awareness of the need for Information Security as an integral part of the day to day business.
- Protecting information assets under the control of the organisation.

**2.3. Scope**

This policy is applicable to and will be communicated to all staff and any third parties who interact with the information held by CRC and all its related information systems. This includes, but is not limited to, any systems or data attached to CRC's computer or telephone networks, systems supplied by CRC or communications sent to or from CRC.

## 3. Responsibilities for Information Security

**3.1.** Ultimate responsibility for the information security policy rests with the Chief Executive Officer (CEO) of the Community Relations Council, with operational responsibility being delegated to the Data Protection Officer, usually being the Director for Finance, Administration and Personnel (DFAP). The DPO shall be responsible for managing and implementing the policy and related procedures.

**3.2.** Line Managers are responsible for ensuring that their permanent staff, temporary workers and other contractors are aware of:

- The information security policies applicable in their work areas.
- Their personal responsibilities for information security; and
- How to access advice on information security matters.

**3.3.** All staff shall comply with information security procedures including the maintenance of data confidentiality and data integrity. Failure to do so may result in disciplinary action.

**3.4.** Line managers shall be individually responsible for the security of their physical environments where information is processed or stored.

**3.5.** Each member of staff shall be responsible for the operational security of the information systems they use.

**3.6.** Each system user shall comply with the security requirements that are currently in force, and shall also ensure that the confidentiality, integrity and availability of the information they use is maintained to the highest standard.

**3.7.** Contracts with external contractors that allow access to the organisation's information systems shall be in operation before access is allowed. These contracts shall ensure that the staff or sub-contractors of the external organisation shall comply with all appropriate security policies

## 4. Legislation

**4.1.** CRC is obliged to abide by all relevant UK and European Union legislation. The requirement to comply with this legislation shall be devolved to employees and agents of CRC, who may be held personally accountable for any breaches of information security for which they may be held responsible. CRC will comply with the following legislation and other legislation as appropriate:

- The Data Protection Act (1998).
- The Data Protection (Processing of Sensitive Personal Data) Order 2000.
- The Copyright, Designs and Patents Act (1988).
- The Computer Misuse Act (1990).
- The Health and Safety at Work Act (1974).
- Human Rights Act (1998).
- Freedom of Information Act 2000.
- General Data Protection Regulation (Regulation (EU) 2016/679 (GDPR).

## 5. Policy Framework

### 5.1. Management of Security

- Day to day responsibility for Information Security shall reside with the DPO.
- The Officer shall be responsible for implementing, monitoring, documenting and communicating security requirements for the organisation.

### 5.2. Information Security Awareness Training

- Information security awareness training shall be included in the staff induction process.
- An ongoing awareness programme shall be established and maintained in order to ensure that staff awareness is refreshed and updated as necessary.

### 5.3. Contracts of Employment

- Staff security requirements shall be addressed at the recruitment stage and all contracts of employment shall contain a confidentiality clause.
- Information security expectations of staff shall be included within appropriate job definitions.

### 5.4. Security Control of Assets

Each IT asset, (hardware, software, application or data) will be tagged and assigned to a specific person.

### 5.5. Access Controls

Only authorised personnel who have a justified and approved business need shall be given access to restricted areas containing information systems or stored data.

**5.6. User Access Controls**

Access to information shall be restricted to authorised users who have a bona-fide business need to access the information.

**5.7. Computer Access Control**

Access to computer facilities shall be restricted to authorised users who have business need to use the facilities.

**5.8. Application Access Control**

Access to data and systems provided by CRC shall be controlled and restricted to those authorised users who have a legitimate business need and permission will be granted to members of staff on a case by case basis.

**5.9. Equipment Security**

In order to minimise loss of, or damage to, all assets, equipment shall be physically protected from threats and environmental hazards.

**5.10. Computer and Network Procedures**

Management of computers and networks shall be controlled through the service level agreement between the Equality Commission for Northern and Ireland and the Community Relations Council.

**5.11. Information Risk Assessment**

The core principle of risk assessment and management requires the identification and quantification of information security risks in terms of their perceived value of asset, severity of impact and the likelihood of occurrence.

Information security risks are recorded within the risk register and action plans are put in place to effectively manage those risks. The risk register and all associated actions are reviewed at regular intervals. Any implemented information security arrangements will also be a regularly reviewed feature of the CRC's risk management programme. These reviews shall help identify areas of continuing best practice and possible weakness, as well as potential risks that may have arisen since the last review was completed.

**5.12. Information security events and weaknesses**

All information security events and suspected weaknesses must be reported to the DPO. All information security events shall be investigated to establish their cause and impacts with a view to avoiding similar events.

### 5.13. Classification of Sensitive Information

In order to safeguard confidentiality, any documents with personally identifiable information:

- should be held securely at all times;
- with only authorised persons should have access;
- should be held only so long as there is a clear business need;
- shall not be left unattended at any time in any place where unauthorised persons might gain access to them; and
- should be transported securely in sealed packaging or locked containers.

The information containing personal information should be held with only one copy in line. However, it is recognised that this may not always be possible. Where an employee understands that personal information is being held twice this should be reported to the DPO. The DPO will then issue a recommendation to the CEO.

This includes sensitive information such as financial and contractual records and should apply to information that the disclosure of which is likely to:

- adversely affect the reputation of the organisation or its staff or cause substantial distress to individuals;
- make it more difficult to maintain the operational effectiveness of the organisation;
- cause financial loss or loss of earning potential, or facilitate improper gain or disadvantage for individuals or organisations;
- prejudice the investigation, or facilitate the commission of crime or other illegal activity;
- breach proper undertakings to maintain the confidence of information provided by third parties or impede the effective development or operation of policies;
- breach statutory restrictions on disclosure of information;
- disadvantage the organisation in commercial or policy negotiations with others or undermine the proper management of the organisation and its operations.

### 5.14. Protection from Malicious Software

CRC will use software countermeasures and management procedures to protect itself against the threat of malicious software. All staff shall be expected to co-operate fully with this policy. Users shall not install software on the organisation's property without permission from the Director of Finance, Administration and Personnel. The Director of Finance, Administration and Personnel will take the advice of the ECNI IT before deciding how to proceed. Users breaching this requirement may be subject to disciplinary action.

### 5.15. User media

Only CRC removable media may be used on CRC's systems. Users breaching this requirement may be subject to disciplinary action.

### 5.16. Email

Emails will only be monitored if CRC has firm evidence that:

- The integrity of the system or the rights of others is under threat.
- The computer regulations are being breached
- Laws are being broken.
- Dishonest practice is occurring.

Email traffic only (not the messages themselves) may be monitored for statistical purposes. Monitoring does not entitle Managers or Administrators to open or read e-mails of other employees without their agreement.

The IT Administrator may be required to gain access to computers in case of emergency or long term or sudden absence, and should this be the case access will be gained using an Administrator password to change the staff member's password to a temporary password which should be changed to a secure password as soon as the staff member returns to their computer.

Authorisation to access files will be the responsibility of the CEO. In an emergency and when the CEO is not available the DPO may grant access. A report must be prepare by the DPO for the CEO at the earliest opportunity. The report must detail why the CEO was unavailable and the reason why the DPO granted access.

Under the new General Data Protection Regulations (GDPR) rules, email addresses will be considered personal data and therefore subject to data protection rules. Therefore as part of developing CRCs data protection email processes to be consistent with the General Data Protection Regulations (GDPR) please:

a) ensure you use Blind Carbon Copy (Bcc) when circulating emails using a CRC mailing list; and
b) consider using Bcc whenever you are sending an email to a third party email with a copy to another third party email. Only use Carbon Copy (CC) where there is a clear reason and basis for doing so.

### 5.17. Accreditation of Information Systems

CRC will ensure that all new information systems, applications and networks include a security plan and are reviewed by ECNI IT and approved by the Programme DFAP Director

### 5.18. System Change Control

Changes to information systems, applications or networks shall be reviewed by ECNI IT and approved by the Programme Director for Finance, Administration and Personnel.

**5.19. Installation of Software**

The organisation shall ensure that all software is properly licensed and approved by the Programme Director for Finance, Administration and Personnel. Users shall not install software on the organisation's property without permission from the Programme Director for Finance, Administration and Personnel. Users breaching this requirement may be subject to disciplinary action.

**5.20. Business Continuity and Disaster Recovery Plans**

CRC will ensure that service continuity plans
include steps to protect applications, systems and networks.

**5.21. Reporting**

The Audit and Risk Assurance Committee will be informed of the information security status of the organisation by means of exception reports.

**5.22. Further Information**

Further information and advice on this policy can be obtained from:

Director for Finance, Administration and Personnel (DPO)
Community Relations Council
2nd Floor, Equality House
7-9 Shaftesbury Square
BELFAST
BT2 7DP