CCEA

Data Protection Policy

Introduction

The Northern Ireland Council for the Curriculum, Examinations and Assessment (CCEA) is committed to compliance with the requirements of the Data Protection Act 1998 (DPA) which came into force on 1 March 2000.

CCEA will aim to ensure that employees, contract staff, council members and partners are fully aware of and abide by their duties and responsibilities under the DPA.

Statement

To operate efficiently CCEA has to collect and use information about people with whom it works. These can include past, current and prospective employees, contracted staff, examination candidates, members of the public, and suppliers.

Personal information must be handled properly, however it is collected, recorded and used, and whether it is in computer or paper records or recorded by other means, for example, photographs or video recording.

CCEA regards the lawful and correct treatment of personal information as critical to its successful operations and to maintaining confidence between it and those with whom it conducts business.

Accordingly CCEA fully endorses and adheres to the Eight Data Protection Principles as set out in the DPA. (see Appendix A)

Disclosure of personal information

Strict conditions apply to the release of personal information both internally and externally. We will not disclose personal information to any third party unless we consider that there is a lawful reason to do so. Respect for confidentiality will be given where appropriate.

In certain circumstances, information relating to staff acting in a business capacity may be disclosed provided there is

- a legal obligation to do so, i.e. we have the statutory power or are required by law to do so; or
- the information is clearly not intrusive in nature; or
- the member of staff has consented to the disclosure; or
- the information is in a form that does not identify individual employees.

Handling of personal and/or sensitive personal information

CCEA will

- observe fully conditions regarding the fair collection and use of personal and sensitive personal information;
- meet its legal obligations to specify the purpose for which personal information is collected and processed;
- collect and process personal information only to the extent that it is needed to fulfil operational needs or to comply with any legal requirements;
- ensure the quality of personal information used;
- apply checks to determine the length of time personal information should be held with reference to the purpose for which it was obtained and any relevant statutory requirements;
- take appropriate technical and organisational security measures to safeguard personal information as outlined in the CCEA Information Security Policy;
- ensure that personal information is not transferred outside of the UK without suitable safeguards;
- respond to subject access requests promptly and within the deadline of 40 calendar days;
- ensure that the rights of people about whom the information is held can be fully exercised under the Act. (see Appendix A)

Compliance

CCEA will ensure that:

- there is someone with specific responsibility for data protection in the organisation;
- all staff managing and handling personal information understand that they are personally responsible for following good data protection practice as well as good records management practice;
- all staff managing and handling personal information are appropriately trained to do so;
- only staff that need access to personal information as part of their duties are authorised to do so;
- queries about handling personal information are promptly and courteously dealt with;
- methods of handling personal information are assessed and evaluated within the organisational business unit or team on an annual basis;
- data sharing with third parties is carried out under a written agreement, setting out the scope and limits of the sharing. Any disclosure of personal information will be in compliance with approved procedures.

Staff Responsibilities

Director of Corporate Services

The Director of Corporate Services (DoCS) is the Senior Information Risk Owner (SIRO) in CCEA. As the SIRO he will:

- ensure CCEA's overall compliance with the DPA;

- have lead responsibility for dealing with data security breaches; and
- ensure that annual training on data protection is made available to all staff.

Business Manager, ICT Services

The Business Manager, ICT Services will act as the SIRO in the absence of the Director of Corporate Services.

Information Officer

The Information Officer will:

- develop and make available best practice guidelines to staff;
- keep CCEA's notification on the Register of Data Controllers up to date;
- provide advice to staff on compliance with the Act, as required;
- carry out compliance checks as agreed with the Business Assurance Manager; and
- develop and deliver annual training for staff.

All Staff

All staff, irrespective of their grade, are responsible for the collection, protection and handling of personal data in their care. They should, therefore, be fully aware of this policy and of their duties under the Act.

They will take steps to ensure that personal data is kept secure at all times against unauthorised or unlawful loss or disclosure or destruction. In particular, they will:

- ensure that paper files and other records or documents containing personal and sensitive personal information are kept in an appropriately secure environment, e.g. lockable cabinets;
- ensure that personal information held on computers and computer systems is protected by the use of secure passwords which are not easily compromised;
- ensure that they are appropriately trained in the handling of personal information;
- not disclose or use personal information held on others for their own purposes;
- ensure that personal data is transported safely between CCEA sites when necessary; and
- notify the Director of Corporate Services, or in his absence the Business Manager ICT Services, of any data losses or breaches, irrespective of the size of the breach or loss.

Contractors and Consultants

All contractors, consultants or partners of CCEA must:

- ensure that they and all of their staff who have access to personal data held or processed for or on behalf of CCEA, are aware of this policy and are fully trained in and are aware of their duties and responsibilities under the DPA.
- allow data protection audits by CCEA of data held on its behalf (if requested).

All third parties who are users of personal information supplied by CCEA will be required to confirm that they will abide by the requirements of the Act with regard to information supplied by CCEA.

Data Breaches

CCEA maintains a Data Security Breach Management Procedure with reference to guidance issued by the Information Commissioner. In the event of a data breach or data loss, staff should notify their Business Manager or Team Leader immediately. He or she will then contact the Director of Corporate Services or, in his absence, the Business Manager ICT Services.

Notification to the Information Commissioner

The Information Commissioner maintains a public register of data controllers. CCEA is registered as such.

The Data Protection Act 1998 requires every data controller who is processing personal data, to notify and renew their notification, on an annual basis. Failure to do so is a criminal offence.

Policy Awareness

A copy of this policy statement will be given to all new members of staff and interested third parties. Existing staff and any relevant third parties will be advised of the policy which will be posted on CCEA's internet and intranet sites, as will any subsequent revisions. All staff and relevant third parties are required to be familiar with and comply with the policy at all times.

Relevant documentation

This policy should be read in conjunction with:

- CCEA Records Management Policy Statement
- CCEA Information Security: Protective Marking, Handling and Disposal Policy (Draft)
- CCEA Subject Access Request Procedure
- Data Protection Staff Guidance
- CCEA Data Security Breach Management Procedure
- CCEA Data Sharing Protocol (Draft)

Appendix A

The Eight Data Protection Principles

The DPA states that anyone processing personal data must comply with the Eight Principles of good practice. These principles are legally enforceable by the Information Commissioner.

The principles require that personal information shall:

1. be processed fairly and lawfully and, in particular, shall not be processed unless specific conditions are met;
2. be obtained only for one or more specified and lawful purposes and shall not be further processed in any manner incompatible with that purpose or those purposes;
3. be adequate, relevant and not excessive in relation to the purpose or purposes for which it is processed;
4. be accurate and where necessary, kept up to date;
5. not be kept for longer than is necessary for that purpose or those purposes;
6. be processed in accordance with the rights of data subjects under the Act;
7. be kept secure i.e. protected by an appropriate degree of security;
8. not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of data protection.

The DPA provides conditions for the processing of any personal data. It also makes a distinction between **personal data** and **"sensitive" personal data**.

Personal data is defined as, data relating to a living individual who can be identified from:

- that data;
- that data and other information which is in the possession of, or is likely to come into the possession of the data controller and includes an expression of opinion about the individual and any indication of the intentions of the data controller, or any other person in respect of the individual.

"Sensitive" personal data is defined as personal data consisting of information as to:

- racial or ethnic origin;
- political opinion;
- religious or other beliefs;
- trade union membership;
- physical or mental health or condition;
- sexual life;
- criminal proceedings or convictions.

The rights of an individual

These include:

- the right to be informed that processing is being undertaken;
- the right of access to one's personal information within the statutory 40 days;
- the right to prevent processing in certain circumstances;

- the right to correct, rectify, block or erase information regarded as wrong information.

Any queries or comments about this policy should be directed to the Information Officer, CCEA, 29 Clarendon Road, Belfast BT1 3BG.

Revision History

Date	Version Number	Prepared by	Approved by	Amendments
30/09/09	1	P Rolleston	N Anderson	
25/02/14	2	P Rolleston	G Byrne	DoCS role and responsibilities amended to include data breach management. Inclusion of role of BUM ICT Services. Section inserted on data breach management. Responsibilities of staff clarified.