

**CCEA**

**Data Protection Policy**

## **Foreward**

The audience for this policy is CCEA staff including permanent staff, contractual staff, temporary and fixed-term staff, customers, stakeholders and the general public.

The purpose of the policy is to set out how CCEA handles personal information and compliance required with data protection legislation.

All staff are required to act within the framework of this 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. Respect for confidentiality should be given where appropriate. In certain circumstances, information relating to staff acting in a business capacity may be made available provided there is

- a legal obligation 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/sensitive information**

CCEA will

- observe fully conditions regarding the fair collection and use of personal information;
- meet its legal obligations to specify the purpose for which information is used;
- collect and process appropriate information only to the extent that it is needed to fulfil operational needs or to comply with any legal requirements;
- ensure the quality of information used;
- apply strict checks to determine the length of time personal information is held;
- take appropriate technical and organisational security measures to safeguard personal information;
- ensure that personal information is not transferred outside of the European Economic Area without suitable safeguards;
- ensure that the rights of people about whom the information is held can be fully exercised under the Act. (see Appendix A)

In addition, CCEA will ensure that:

- there is someone with specific responsibility for data protection in the organisation;
- everyone managing and handling personal information understands that they are contractually responsible for good data protection practice;
- everyone managing and handling personal information is appropriately trained to do so;
- queries about handling personal information are promptly and courteously dealt with;
- methods of handling personal information are regularly assessed and evaluated;
- performance with handling personal information is regularly assessed and evaluated;
- data sharing is carried out under a written agreement, setting out the scope and limits of the sharing. Any disclosure of personal data will be in compliance with approved procedures.

## **Staff Responsibilities**

All staff have responsibility for the protection of personal data and should, therefore, be made 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 and in particular will ensure that:

- paper files and other records or documents containing personal/sensitive data are kept in a secure environment;
- personal data held on computers and computer systems is protected by the use of secure passwords which, where possible, have “forced” changes periodically;
- individual passwords should be such that they are not easily compromised.

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 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.

## **Implementation**

In CCEA responsibility for ensuring compliance with the Data Protection Act rests with the Director of Corporate Services. The Information Officer who works in the Business Assurance Unit has delegated responsibility for:

- the development of best practice guidelines; and
- carrying out compliance checks to ensure adherence, throughout CCEA, with the Data Protection Act.

## **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.

To this end the Information Officer will be responsible for collating information relating to the processing of personal data within CCEA.

The Information Officer will review the Data Protection Register prior to notification to the Information Commissioner.

Any changes to the register will be notified to the Information Commissioner, within 28 days.

To this end, any changes made between reviews should be brought to the attention of the Information Officer immediately.

## **Policy Awareness**

A copy of this policy statement will be brought to the attention of 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

Version 1.0

will any subsequent revisions. All staff and relevant third parties are required to be familiar with and comply with the policy at all times.

## 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;

Version 1.0

- 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.