Rewarding Learning

Business Assurance

Data Protection Policy

Introduction

The Data Protection Act (DPA) 2018 applies GDPR standards but it has been amended to adjust those that would not work in the national context. The Northern Ireland Council for the Curriculum, Examinations and Assessment (CCEA) is committed to compliance with the requirements of the Data Protection Act 2018 (DPA) including the General Data Protection Regulation (GDPR) which came into effect on the 25th May 2018.

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, however, there may be explicit references to the GDPR for clarity. Appendix B provides definitions for key definitions to assist users of this policy in understanding key concepts.

Statement

In order to operate effectively and 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 7 Key Data Protection Principles as set out in the GDPR (see Appendix A). Full details of CCEA's compliance with the 7 principles can be found in the published Privacy Notice which can be accessed via the link : http://ccea.org.uk/legal/privacy_policy. The CCEA Privacy Notice also contain details of the legal basis under which CCEA processes personal information.

Disclosure of personal information

Strict conditions apply to the release of personal information both internally and externally. CCEA 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. This includes ensuring that hard copy personal data is dispatched securely through use of CCEA's contracted courier service which provides full tracking of individual packages. Where possible dispatch of hard copy personal data will be organised through the Distribution Team Manager.
- ensure that personal information is not transferred outside of the UK without suitable safeguards;
- respond to subject access requests in line with the CCEA Team Procedure for Processing Subject Access Requests; and
- ensure that the rights of people about whom the information is held can be fully exercised under the DPA (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; and
- 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 Finance and Corporate Services

The Director of Finance and Corporate Services (DoFCS) is the Senior Information Risk Owner (SIRO) in CCEA. As the SIRO he/she will:

- ensure CCEA's overall compliance with the GDPR and the DPA;

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

Data Protection Officer (DPO)

CCEA's DPO is David Wilson, Business Assurance Manager. The DPO 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 required; and
- develop and ensure delivery of appropriate 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 DPA.

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 and external venues when necessary; and
- notify the Director of Finance and Corporate 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 DPA with regard to information supplied by CCEA.

Data Breaches

CCEA has developed a Team Procedure for the Management of Data Breaches/ Losses which is consistent with the guidance issued by the Information

Commissioner's Office (ICO). In the event of a data breach/loss, staff should notify their Business Manager/Team Leader immediately. He/she will then contact the Director of Finance and Corporate Services. All reported data breaches/losses will be handled in line with the Team Procedure for the Management of Data Breaches/Losses and will be formally recorded by the DPO.

Notification to the Information Commissioner's Office (ICO)

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

Where a data breach is assessed to have a likely risk to the rights/freedoms of individuals, CCEA will report the breach to the ICO within 72 hours of being made aware of the breach.

Policy Awareness

This policy will be provided to all new members of staff and interested third parties. Existing staff and any relevant third parties will be made aware 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:

- ICO Overview of the General Data Protection Regulation (GDPR)
- CCEA Records Management Policy Statement
- CCEA Information Security: Protective Marking, Handling and Disposal Policy
- CCEA Team Procedure for Processing Subject Access Requests
- CCEA Data Sharing Protocol
- CCEA Team Procedure for the Management of Data Breaches/Losses
- CCEA Privacy Notice

Appendix A

The Seven Key Principles of Data Protection

The GDPR states that anyone processing personal data must comply with the 7 Key Principles of Data Protection. These principles are legally enforceable by the Information Commissioner.

The principles require that personal information shall be:

(a) processed lawfully, fairly and in a transparent manner in relation to individuals ('lawfulness, fairness and transparency');

(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes ('purpose limitation');

(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');

(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals ('storage limitation');

(f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality')."

(g) the controller shall be responsible for, and be able to demonstrate compliance and 'accountability'.

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

Failure to comply with the principles may leave you open to substantial fines. Article 83(5)(a) states that infringements of the basic principles for processing personal data are subject to the highest tier of administrative fines. This could mean a fine of up to €20 million, or 4% of your total worldwide annual turnover, whichever is higher.

The rights of an individual

These include:

- **the right to be informed**: CCEA shall keep data subjects informed of its processing activities through its Privacy Notice;
- **the right of access**: a data subject may request access to the Personal Data which CCEA holds about them (i.e. a SAR);

- **the right to rectification**: if a data subject informs CCEA that Personal Data held by CCEA is inaccurate or incomplete, the data subject may request that it is rectified;
- **the right to erasure**: a data subject may ask CCEA to erase their Personal Data. CCEA must comply with this request unless it has reasonable grounds to refuse;
- **the right to data portability**: a data subject is entitled to receive a copy of their Personal Data and use it for other purposes;
- **the right to object**: a data subject may object to CCEA's processing of their Personal Data at any time;
- **rights in relation to automated decision-making and profiling**: a data subject has the right to challenge any decision that is made about them on an automated basis (subject to certain exceptions). CCEA is also required to comply with certain conditions if it uses Personal Data for profiling purposes.

Any queries regarding this policy should be directed to David Wilson, Data Protection Officer, CCEA, 29 Clarendon Road, Belfast BT1 3BG. CCEA reserves the right to amend this policy without notice for example for legislative or operational reasons.

Appendix B

Useful Definitions

Term	Definition
Personal data	Personal data is defined as, data relating to a living individual who are identifiable directly from the information in question or from that information in combination with other information. Personal data may also include special categories of personal data or criminal conviction and offences data. These are considered to be more sensitive and you may only process them in more limited circumstances.
Sensitive Personal Data	Personal data may also include special categories of personal data or criminal conviction and offences data. These are considered to be more sensitive and you may only process them in more limited circumstances. Sensitive personal data categories are as follows ; racial or ethnic origin; political opinion; religious or other beliefs; trade union membership; physical or mental health or condition; sexual life; and criminal proceedings or convictions.
Data Controller	The person (or business) who determines the purposes for which, and the way in which, personal data is processed.
Data Processor	Anyone who processes personal data on behalf of the data controller (excluding the data controller's own employees).
Data Processing	An operation or set of operations which is performed on information, or on sets of information, such as the : collection, recording, organisation, structuring or storage ; adaptation or alteration ; retrieval, consultation or use ; disclosure by transmission, dissemination or otherwise making available; alignment or combination; or restriction, erasure or destruction.
Data Subject	The identified or identifiable living individual to whom personal data relates.

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.
14/06/18	3		G.Byrne	To update in line with DPA (2018) which applies GDPR
October 2018	4	D. Wilson	L. Scott	Updated to reflect changing responsibilities/terminology.
December 2018	5	D. Wilson	J. Daly	Updated to take account of consultation feedback.
March 2019	6	D. Wilson	Finance Committee	Updated to reflect legal advice received.