Data Protection Policy

INTRODUCTION

The following information on data protection should be read in conjunction with the Data Protection Policy on the CDN website and the Personal Information and Security Policy. Both policies can be found on the CDN drive (please see the Corporate Services Manager for further information).

CDN is fully committed to compliance with the requirements of the UK General Data Protection Regulation, the Data Protection Act 2018 and all other data protection legislation currently in force. Data Protection Law applies to any organisation processing personal data. It sets out principles which should be followed and gives rights to those whose data is being processed.

SCOPE

This policy applies to all CDN staff and contractors and all items of personal data that are processed through any activity of CDN.

The definition of 'processing data' includes obtaining/collecting, recording, holding, storing, organising, adapting, aligning, copying, transferring, combining, blocking, erasing and destroying the information or data. It also includes carrying out any operation or set of operations.

ROLES AND RESPONSIBILITIES

All staff:

- All staff must undertake the data protection training required for their roles.
- All personal data must be handled safely and securely, according to the CDN's agreed policies**,** and the data protection principles (see below).
- Personal data must be processed in a fair and lawful way. This means that personal data should only be processed if we have a valid lawful basis and purpose for processing (eg. a contract with the data subject, or a legal obligation) and we have provided information to the individuals concerned about how and why we are processing their information (i.e. a privacy notice). See the CDN's **Record of Processing Procedure** and **Privacy Notice Procedure.**
- Restrictions on processing personal data must be adhered to, such as not passing personal data on to third parties, not transferring data outside the UK and not using it for direct marketing, unless particular conditions are in place.
- Personal data must not be disclosed to any unauthorised third party, in any form, either accidentally or otherwise. Data must only be shared in line with the CDN's **Data Sharing/Data Processor Procedure.**
- Any staff member who becomes aware of a personal data breach must report it immediately. Find details of how to report a breach in the **Breach Management Procedure**.

- Any deliberate breach of this policy may lead to disciplinary action being taken, access to CDN facilities being withdrawn, or even criminal prosecution. Staff may also incur criminal liability if they knowingly or recklessly obtain and/or disclose personal information without the consent of the CDN, ie. for their own purposes, which are outside the legitimate purposes of the CDN.

Staff developing new projects/processes or revising existing processes

- Data protection must be taken into account and data protection screening undertaken to determine the need to carry out a Data Protection Impact Assessment (DPIA). Find details of how to undertake DPIA screening and assessment in the **DPIA Procedure**. Consult the Data Protection Officer for advice.

- Inform the Data Protection Officer before starting any new activity which is not covered by one of the existing Records of Processing Activities (ROPA).

- Understand that the processing of data about children has certain restrictions in data protection law and consult the Data Protection Officer before embarking on any new processing of personal data involving children.

Data Protection Officer

- Monitors the CDN's compliance with UK data protection law.
- Advises the CDN on compliance with UK data protection law.
- Acts as the point of contact for the public and the Information Commissioner's Office (ICO) for consultation, enquiries, and the management of breach reporting.

Senior Leadership Team

- Receive reports from the Data Protection Officer.
- Hold accountability for the CDN's compliance with the provisions of UK data protection law.
- Have oversight of the documentation of processing activities in the CDN's ROPA and oversight of DPIAs and associated actions.

As a data controller the CDN is required to maintain a ROPA which covers all the processing of personal data carried out by the CDN. The ROPA details why personal data is being processed, the types of individuals about which information is held, who the personal information is shared with and when personal information is transferred to countries outside the UK.

THE DATA PROTECTION PRINCIPLES

To this end, CDN endorses fully and adheres to the Data Protection Principles listed below. When processing data we will ensure that it is:

- processed lawfully, fairly and in a transparent way ('lawfulness, fairness and transparency')
- processed no further than the legitimate purposes for which that data was collected ('purpose limitation')
- limited to what is necessary in relation to the purpose ('data minimisation')
- accurate and kept up to date ('accuracy')

- kept in a form which permits identification of the data subject for no longer than is necessary ('storage limitation')
- processed in a manner that ensures security of that personal data ('integrity and confidentiality')
- processed by a controller who can demonstrate compliance with the principles ('accountability').

These principles must be observed at all times when processing or using personal information. Therefore, through appropriate management and strict application of criteria and controls, CDN will:

- observe fully the conditions regarding having a lawful basis to process personal information
- meet its legal obligations to specify the purposes for which information is used
- collect and process appropriate information only to the extent that it is necessary to fulfil operational needs or to comply with any legal requirements
- ensure the information held is accurate and up to date
- ensure that the information is held for no longer than is necessary
- ensure that the rights of people about whom information is held can be fully exercised under the Data Protection Act 2018 (i.e. the right to be informed that processing is being undertaken, to access personal information on request; to prevent processing in certain circumstances, and to correct, rectify, block or erase information that is regarded as wrong information)
- take appropriate technical and organisational security measures to safeguard personal information
- ensure that personal information is not transferred outside the EU, to other countries or international organisations without an adequate level of protection or consent

DATA SUBJECT'S RIGHTS

UK GDPR gives data subjects the right to access personal information held about them by the CDN. The purpose of a subject access request is to allow individuals to confirm the accuracy of personal data and check the lawfulness of processing to allow them to exercise rights of correction or objection if necessary. However, individuals can request to see any information that the CDN holds about them which includes copies of email correspondence referring to them or opinions expressed about them.

The CDN will respond to all requests for personal information and information will normally be provided free of charge.

The CDN will uphold the following rights of data subjects under UK GDPR:

- **Right to Access** – the right to access personal information, where this is not limited by exemptions the CDN may apply based on the balance of interests in providing access to the information.

- **Right to Object** – the right to object to specific types of processing including processing for direct marketing. The data subject needs to demonstrate grounds for objecting to the processing relating to their particular situation, except in the case of direct marketing where it is an absolute right (see **Direct Marketing Procedure**). Online services must offer an automated method of objecting. In some cases, there may be an exemption to this right for research or statistical purposes done in the public interest.

- **Right to be forgotten (erasure)** – the right for individuals to have their data erased in certain situations, such as where the data is no longer required for the purpose it was collected, the individual withdraws consent, or the information is being processed unlawfully.

- There is an exemption to this for scientific or historical research purposes or statistical purposes if the erasure would render impossible or seriously impair the achievement of the objectives of the research. Individuals can ask the controller to 'restrict' processing of the data whilst complaints (for example, about accuracy) are resolved or the processing is unlawful.

- **Rights in relation to automated decision making and profiling** – The right relates to automated decisions or profiling that could result in significant affects to an individual. Profiling is the processing of data to evaluate, analyse or predict behaviour or any feature of their behaviour, preferences or identity. Individuals have the right not to be subject to decisions based solely on automated processing. When profiling is used, measures must be put in place to ensure security and reliability of services. Automated decision-taking based on sensitive data can only be done with explicit consent.

- **Right to Rectification** – the right to require a controller to rectify inaccuracies in personal data held about them. In some circumstances, if personal data is incomplete, an individual can require the controller to complete the data, or to record a supplementary statement.

- **Right to Portability** – the right to request personal information is provided in a structured, commonly used and machine readable form so it can be sent to another data controller. This only applies to personal data that is processed by automated means (not paper records); to personal data which the data subject has provided to the controller, and only when it is being processed on the basis of consent or a contract.

- **Right to Restrict Processing** – this right will generally be exercised in line with one of the other rights, such as an objection or seeking to have personal data deleted. The CDN may restrict the processing of personal data in response to a request where this is justified in the circumstances of the case.

The availability of data subject rights largely depends on the lawful basis for processing. The table below summarises when rights are available.

	Lawful Basis for Processing					
Data Subject Right	Consent	Contract	Legal Obligation	Vital Interests	Public Task	Legitimate Interests
Access	Yes	Yes	Yes	Yes	Yes	Yes
Erasure	Yes	Yes	No	Yes	No	Yes
Restrict Processing	Yes	Yes	Yes	Yes	Yes	Yes
Rectification	Yes	Yes	Yes	Yes	Yes	Yes
Portability	Yes	Yes	No	No	No	No

Object	No but can withdraw consent	No	No	No	Yes	Yes
Automated Decision	Yes	Yes	Yes	Yes	Yes	Yes

The UK Data Protection Act 2018 provides exemptions to data subject rights in certain circumstances. The CDN may be exempt from compliance with data subject rights where these exemptions apply. Careful consideration should be given to exemptions before responding to any request by a data subject. See the **Data Subject Rights Requests Procedure**.

Any requests made to invoke any of the rights above will be dealt with promptly and in any case within one month of receiving the request, unless the request is particularly complex in which case an extension of a period of up to two months may be applied. Members of staff should consult the Information/Data Protection Team on info@cdn.ac.uk if any requests like these are received.

DATA SECURITY

You are responsible for ensuring that any personal data that you hold and/or process as part of your job role is stored securely.

You must ensure that personal information is not disclosed either orally or in writing, or via web pages, or by any other means, accidentally or otherwise, to any unauthorised third party.

You should note that unauthorised disclosure may result in action under the disciplinary procedure, which may include dismissal for gross misconduct. Personal information should be kept in a locked filing cabinet, drawer, or safe. Electronic data should be coded, encrypted, or password protected both on a local hard drive and on a network drive that is regularly backed up. If a copy is kept on removable storage media, that media must itself be kept in a locked filing cabinet, drawer or safe.

When travelling with a device containing personal data, you must ensure both the device and data are password protected. The device should be kept secure and where possible it should be locked away out of sight ie. in the boot of a car. You should avoid travelling with hard copies of personal data where there is secure electronic storage available. When it is essential to travel with hard copies of personal data this should be kept securely in a bag and where possible locked away out of sight ie. in the boot of a car.

NOTIFYING BREACHES

A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or processed. See further details in the Personal Data Breach Management Procedure.

The following are examples of data breaches:
a) access by an unauthorised third party;
b) deliberate or accidental action (or inaction) by a data controller or data processor;

c) sending personal data to an incorrect recipient;
d) computing devices containing personal data being lost or stolen;
e) alteration of personal data without permission;
f) loss of availability of personal data.

INVESTIGATION AND NOTIFICATION

If a member of staff thinks they may have breached this policy, they should report this to info@cdn.ac.uk immediately.

Quick action can be crucial in mitigating the negative effects of a breach, in particular where data security is concerned; it is therefore vital that members of staff raise the issue immediately in accordance with this policy.

In the event that we become aware of a breach, or a potential breach, an investigation will be carried out. This investigation will be carried out by the Head of Marketing & Development and the Data Protection Officer.

We will undertake to notify the Information Commissioner of a breach which is likely to pose a risk to people's rights and freedoms without undue delay and at the latest within 72 hours of discovery. If we are unable to report in full within this timescale, we will make an initial report to the Information Commissioner, and then provide a full report in more than one instalment if so required.

We will undertake to notify the individual whose data is the subject of a breach if there is a high risk to people's rights and freedoms without undue delay and may, dependent on the circumstances, be made before the supervisory authority is notified.

RECORD OF BREACHES

CDN records all personal data breaches regardless of whether they are notifiable or not as part of its general accountability requirement under UK GDPR. It records the facts relating to the breach, its effects and the remedial action taken.

HOW WILL WE KNOW IF THIS POLICY IS WORKING?

The CDN will monitor compliance with this policy and associated procedures by using management registers to document processing activities. Statistics and anonymous information may be provided to senior management and auditors based on the content of the registers.

HOW WILL WE KEEP THIS POLICY UP TO DATE?

The policy will be subject to an annual review cycle.

ASSOCIATED PROCEDURES

The following associated procedures should be consulted in conjunction with the Data Protection Policy as appropriate.

- Privacy Notices
- Personal Data Breach Management
- Record of Processing Activities (ROPA)
- Data Protection Impact Assessments (DPIAs)

- Data Subject Rights Requests
- Data Sharing / Data Processor
- Police Requests for Personal Data
- Direct Marketing
- International Transfers of Personal Data
- Research.

CDN CONTACTS

The CDN's named Data Protection Officer may be contacted at info@cdn.ac.uk.

In the first instance all enquiries or requests for further information or guidance relating to data protection should be addressed to the Data Protection Officer.

DEFINITIONS

- **Personal Data** – information relating to an identifiable living person ('**data subject**')
- **Special Category Data** – information relating to racial or ethnic origin, political opinions, religious or philosophical beliefs, Trade Union membership, genetic and biometric data used to identify an individual, health data, sex life data, sexual orientation.
- **Criminal Convictions Data** – data processed relating to criminal convictions and offences, or related security measures
- **Processing** – any operation or set of operations carried out on personal data including recording, organisation, storage, adaptation or alteration, retrieval, consultation, disclosure by transmission, dissemination, erasure or destruction.
- **Profiling** – automated processing of personal data to evaluate certain personal aspects relating to a person, in particular to analyse or predict aspects concerning that person's performance at work, economic situation, health, personal preferences, reliability, behaviour or movements.
- **Controller** – organisation, person or other body which alone or jointly with others, determines the purpose and means of processing of personal data.
- **Processor** – organisation, person or other body which processes personal data on behalf of the controller.
- **Third party** – organisation, person or other body, other than the data subject, controller or processor.
- **Personal data breach** – beach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

APPENDIX – SPECIAL CATEGORY AND CRIMINAL CONVICTIONS DATA

Special category data will be processed by the CDN for a number of reasons related to, and not incompatible with, the specified purpose for which it was originally collected.

Employee Data	
Purpose of Processing	**Lawful Basis**
Sickness Absence	• UK GDPR Article 6(1)(b) - performance of a contract • UK GDPR Article 9(2)(g) – reasons of substantial public interest

	• DPA 2018, Schedule 1, Part 1, 2. Health and Social care purposes (b) assessment of the working capacity of an employee (Employment Rights Act 1996)
Occupational health	• UK GDPR Article 6(1)(b) – performance of a contract • UK GDPR Article 9(2)(h) – occupational medicine and assessment of working capacity of an employee • DPA 2018, Schedule 1, Part 1, 2. Health and Social Care purposes (a) occupational medicine and (b) assessment of working capacity of an employee. (Health and Safety at Work etc. Act 1974)
Disciplinary and grievance procedures	• UK GDPR Article 6(1)(b) – performance of a contract • UK GDPR Article 9(2)(b) – employment law • DPA 2018, Schedule 1, Part 2, 11 protecting the public against dishonesty etc. (2)(a) – protect members of the public against dishonesty, malpractice, or other seriously improper conduct (Employment Rights Act 1996)
Trade Union membership data	• UK GDPR Article 6(1)(b) – performance of a contract • UK GDPR Article 9(2)(b) – employment and social protection law • DPA 2018, Schedule 1, Part 2, 6. (2)(a) – exercise of a function conferred by an enactment or rule of law (Trade Union and Labour Relations (Consolidation) Act 1992)
Equality and diversity data	• UK GDPR Article 6(1)(c) – legal obligation • UK GDPR Article 9(2)(g) – reasons of substantial public interest • DPA 2018, Schedule 1, Part 2, 8. (1) – equality or opportunity of treatment (Equality Act 2010)
Protected Disclosures	• UK GDPR Article 6(1)(c) – legal obligation • UK GDPR Article 9(2)(g) – reasons of substantial public interest • DPA 2018, Schedule 1, Part 2, 6. (2)(a) – exercise of a function conferred by an enactment or rule of law (Employment Rights Act 1996, Public Interest Disclosure Act 1998)

Learner Data	
Purpose of Processing	**Lawful Basis**
Equality and diversity data	• UK GDPR Article 6(1)(c) – legal obligation • UK GDPR Article 9(2)(g) – reasons of substantial public interest • DPA 2018, Schedule 1, Part 2, 8. (1) – equality or opportunity of treatment (Equality Act 2010)
Provision of additional support	• UK GDPR Article 6(1)(c) – legal obligation • UK GDPR Article 9(2)(g) - reasons of substantial public interest • DPA 2018, Sch 1, Part 2, 16 – support for individuals with a particular disability or medical condition (Equality Act 2010)