huish | POLICIES

Author | Laura Rice
Contributors | Richard Anderson
Version | 0.1
Pages | 8
Publication Date | Awaiting Corporation Approval
Last Review Date | 22/05/2018
Next Review Date | 22/05/2019

Data Protection and Information Security Policy

CONTENTS

1. INTRODUCTION AND DATA PROTECTION PRINCIPLES

This policy sets out the College's obligations under Data Protection legislation, including the General Data Protection Regulation and Act. The provision contained within this Policy applies to all students, staff and other individuals for whom the College may hold personal data or who may process personal data held on behalf of the College.

The College collects and uses information about those with whom it works, including information about employees, students, applicants, parents/guardians of students and details of other external stakeholders. As a public entity, the College uses information to enable the fulfilment of contractual agreements with government funding agencies and carrying out its day-to-day business. In carrying out its business, the College meets statutory obligations and seeks to follow best practice in the principles of data protection.

The College will follow the key principles of data protection to ensure that data will be:

i. Processed securely, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures
ii. Processed fairly and lawfully in a transparent manner
iii. Processed for one or more specified, explicit and legitimate purpose/s
iv. Adequate, relevant and limited to what is necessary
v. Accurate and where necessary, kept up-to-date
vi. Kept in a form that permits identification of data subject for no longer than is necessary

2. SCOPE AND CATEGORISATION OF DATA

The scope of this Policy includes all College activities involving the processing of personal or sensitive data as defined below, including images and text, from which a living individual person can be identified. This includes personal or sensitive data held in a computer system or in a structured manual filing system. Data in the College is categorised according to the following definitions:

2.1 Personal Data - Any information relating to an identified or identifiable natural personal. This can be direct or indirect identification and is technologically neutral.

2.2 Sensitive Personal Data

- Racial or ethnic origin
- Political beliefs
- Religious or philosophical beliefs
- Trade Union membership
- Genetic or biometric data
- Physical or mental health
- Sexual orientation
- Criminal Records

2.3 Non-Personal Data

Non-personal data can be either confidential or non-confidential information. Confidential information consists of information that, if disclosed or made public, could damage the College's commercial or financial interests or reputation; or cause the College to not meet its legal obligations. The definition of 'confidential' includes any information that either is labelled as 'confidential' or, if not labelled 'confidential', would nevertheless be reasonably regarded as confidential.

3. RESPONSIBILITIES

The College is the 'Data Controller' in that it determines the need to collect data. Day-to-day responsibility for management and implementation of relevant Data Protection legislation and policies lies with the Principal and the appointed Data Protection Officer.

Every member of staff, governors and others associated with the College, including temporary or agency staff, volunteers or contractors working for or on behalf of the College, have an individual and collective responsibility to uphold the provision contained in this Policy and related documents.

3.1 Data Protection Officer

The College Data Protection Officer (DPO), reports to the Principal and plays a key role in fostering a culture of data awareness and protection within the College. The DPO will provide advice and guidance on the interpretation and implementation of data protection controls and measures to ensure compliance with relevant legislation.

The email address for any data protection queries relating to staff or students is:

dataprotection@richuish.ac.uk

3.2 Ethos and Culture of Data Protection

All staff have a responsibility to check that any information they provide to the College in connection with their employment is accurate and up-to-date and that they inform the College of any errors or changes.

All staff have a responsibility to ensure the secure keeping of any personal data they handle, whether in electronic or paper format.

The College encourages staff to raise questions about data protection matters and to report any issues or data breaches as soon as practically possible.

The College will ensure that staff receive appropriate training and development to ensure that everyone understands their responsibilities under this Policy.

3.3 Students

All students, whatever their type/level of enrolment, must provide personal data as required by the College in order to fulfil its public task to provide educational services. Students have a responsibility to keep this information up-to-date and inform the College of any changes by emailing cis@richuish.ac.uk

4. DATA PROTECTION RECORDS

4.1 Data Register and Retention Schedules

The College Data Protection Officer must keep the following records:

- The number, processing timescales and nature of Subject Access Requests, along with all correspondence.
- The number, processing timescales and nature of any other requests relating to individual rights as covered in the GDPR.
- The number, nature and related timescales of identified data breaches, supplemented with details of consequent investigations, recommendations and audits.
- Copies of Data Protection Impact Assessments, and related audits.
- Full detail of any communications with the Information Commissioner's Office

5. FAIR AND LAWFUL PROCESSING

All Personal data held by the College will be processed and stored in a lawful, fair and transparent manner. The data will be kept safe from unauthorised access or accidental loss. The data will only be kept for as long as needed for proper purposes.

5.1 Legal Bases

The College will identify the legal basis for processing personal data in the Data Register and Retention Schedules. The GDPR identifies the options as follows:

- The data subject has given consent to the processing of his or her personal data for one or more specific purposes;
- Processing is necessary for the performance of a contract to which the data subject is party
- Processing is necessary for compliance with the College's legal obligation
- Processing is necessary in order to protect the vital interests of the data subject or other person;
- Processing is necessary for the performance of a task carried out in the public interest;
- Processing is necessary for the purposes of the legitimate interests pursued by the College

5.2 Use of Consent as legal basis for processing personal data

Where consent is identified as the legal basis for processing personal data, the College will ensure that evidence is available to demonstrate that consent has been given. In all cases when consent is requested, this will be in an intelligible and easily accessible form, using clear and plain language. An individual will be given opportunities to withdraw consent and College processes and systems will make this possible.

Where consent is the legal basis for processing personal data, this must be collected via a clear affirmative act, being freely given, specific, informed and an unambiguous indication of the individual's agreement to processing related to him or her.

5.3 CCTV

The College will ensure that all legal obligations are met when using CCTV. This includes acting in accordance with Data Protection legislation, the Freedom of Information Act 2000, the Protection of Freedoms Act 2012 and the Human Rights Act 1998.

5.4 Quality of personal data

As far as reasonably possible, the College will ensure that personal data is kept up-to-date and accurate.

5.5 Privacy Notices

The College will implement privacy notices and will provide the College details (as data controller), the contact details of the College Data Protection Officer, the purposes of data processing (how data

is used), how it is stored, the legal bases for data processing, categories or what categories of people will receive or have access to the data and individual's rights.

The College will use clear and plain language in all cases.

6. TECHNICAL AND ORGANISATION MEASURES

The College will uphold the principle of integrity and confidentiality of personal data processing.

6.1 Physical and Environmental Security Measures

The processing of personal data by the College will be subject to appropriate physical and environmental security measures.

6.2 Data Sharing

The College will ensure that appropriate Data Sharing Agreements are in place.

6.3 Data in transit

The College will ensure that staff understand the requirement for the security and safety of personal, sensitive or confidential business critical data when transferring to or from a third party.

6.4 IT Security

The College will ensure that appropriate policies, systems and procedures are in place, including an IT Acceptable Use Policy, to ensure the security of its IT network, including College owned devices for use off site and public devices accessing College systems.

The College will appropriately assess network security and vulnerability according to legislation and best practice.

6.6 Data Protection by design and Data Protection Impact Assessments (DPIAs)

The College has a responsibility to assess the risks to the safety and security of personal data at the early stages of any project or initiative. This will enable the early identification of potential issues and consideration of measures to address identified risks.

7. DATA BREACHES

A personal data breach is defined as a breach of security leading to the inappropriate destruction, loss, alteration, unauthorised disclosure of, or access to, personal data either in physical or electronic format.

Through the work of the Data Protection Officer, staff should feel supported in their work and able to access timely and appropriate guidance/support to enable the secure handling and processing of personal data.

In the event of any data breach, the College will conduct an investigation and may invoke the College Disciplinary Policy.

The College will ensure that all staff are aware of what constitutes a personal data breach, and their responsibilities to report any such incident.

8. INDIVIDUAL RIGHTS

8.1 Subject Access Rights

Under the provision of Data Protection legislation, staff, students and other individuals have the right to access any personal data processed by the College, whether in electronic or paper format.

Any person wishing to exercise this right must make a request in writing to the College's Data Protection Officer. The College, via the DPO, will comply with requests for access to personal data as quickly as possible and without undue delay, but will ensure that a response is given within one month of receipt of the request. That period may be extended by two further months when necessary.

Information will be provided free of charge. When a request is manifestly unfounded or excessive, the College may charge a reasonable fee, taking into account the costs of providing the information, or may refuse to act on the request.

8.2 Other Individual Rights

Under Data Protection legislation, an individual has specific rights relating to their personal data processed by the College. In some circumstances, the College may apply some restrictions to these and the advice of the College's Data Protection Officer must always be sought to ensure full compliance with relevant legislation.

Individual rights include:

- **Right to rectification –** right to rectification of inaccurate personal data processed by the College, concerning him or her
- **Right to erasure** – the right, in some circumstances to require the College to erase personal data concerning him or her.
- **Right to data portability –** the right , in some circumstances, to have personal data concerning him or her transmitted to another data controller
- **Right to object –** the right to object, in some circumstances, to the processing of personal data concerning him or her, on grounds relating to his or her situation
- **Rights relating to automated decision-**making and profiling – the right not to be subject to a decision based solely on automated processing, including profiling, in certain situations.

Enquiries about this Policy

Any enquiries about the provision and content of this Policy should be made to the Data Protection Officer.