co-operative college

| | | |
|---|---|---|
| **Policy Type** | HR/People Policy | |
| **Title** | Data Protection Policy | |
| **Aim** | To comply with the requirements of the Data Protection Act 1998 and the General Data Protection Regulation (GDPR).<br><br>To minimise any risk to the Co-operative College, by setting out clear guidelines relating to the processing, storage and disposal of data.<br><br>To ensure the rights of Data Subjects are clear and the process of exercising those rights are explained. | |
| **Scope** | All employees and workers who handle personal data, whether this relates to their colleagues, the College or anyone else.<br><br>All Members, Associates, Trustees and Learners whose data is processed by the Co-operative College.<br><br>A copy will also be given to any third parties to whom we outsource any data processing or storage. | |
| **Related Policies / Documents / Procedures** | The Data Protection Policy is related to many of the College's other policies, but in particular to:<br>• IT and Computer Use Policy | |
| **Date for Implementation** | Immediately after approval | |
| **Approved by** | CEO & Principal<br>Board of Trustees | November 2021 |
| | Union Representative | May 2018 |
| **Date of next review** | November 2022 | |
| **Date of last review** | November 2021 | |
| **Reviewed by** | RS Baxter Consulting | |

| | |
|---|---|
| **Distribution** | All College staff |
| **Version Control** | **Previous Versions approved:**<br>March 2008<br>March 2016<br>May 2018<br>April 2020 |

## Introduction

The Co-operative College holds information about its board members; current, past and prospective employees; learners; partner organisations; suppliers and other users as a normal part of its day-to-day business. It is necessary for example to process information so that staff can be recruited and paid, learners enrolled, courses organised, awards and assessments held and legal obligations to funding bodies and government complied with. Personal data may consist of data kept on paper, computer or other electronic media; all of which is protected under the Data Protection Act 1998 and General Data Protection Regulation.

The Co-operative College and all staff or others who process or use personal information must ensure that they follow the Data Protection Principles at all times. In order to ensure that this happens, the Co-operative College has developed this Data Protection Policy.

### *Purpose*

The Co-operative College is committed to being transparent about how it collects and uses personal data, and to meeting its data protection obligations. This policy sets out the organisation's commitment to data protection, and individual rights and obligations in relation to personal data.

This policy applies to the personal data of job applicants, employees, Board Members, Associates, volunteers, interns, apprentices, former employees, members, learners, partner organisations, clients/customers and suppliers. The College has adopted a broad approach to Data Protection, applying the same principles across the organisation.

The organisation has appointed the Learning Technologist as the person with responsibility for data protection compliance within the organisation. They can be contacted at data@co-op.ac.uk. Questions about this policy, or requests for further information, should be directed to them.

### *Definitions*

**"Personal data"** is any information that relates to an individual who can be identified from that information. Processing is any use that is made of data, including collecting, storing, amending, disclosing or destroying it.

**"Special categories of personal data"** means information about an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life or sexual orientation and biometric data.

**"Criminal records data"** means information about an individual's criminal convictions and offences, and information relating to criminal allegations and proceedings.

**"The organisation"** refers to The Co-operative College.

## Data Protection Principles

The Co-operative College processes personal data in accordance with the following data protection principles:

- The organisation processes personal data lawfully, fairly and in a transparent manner.
- The organisation collects personal data only for specified, explicit and legitimate purposes.
- The organisation processes personal data only where it is adequate, relevant and limited to what is necessary for the purposes of processing.
- The organisation keeps accurate personal data and takes all reasonable steps to ensure that inaccurate personal data is rectified or deleted without delay.
- The organisation keeps personal data only for the period necessary for processing.
- The organisation adopts appropriate measures to make sure that personal data is secure, and protected against unauthorised or unlawful processing, and accidental loss, destruction or damage.

The organisation tells individuals the reasons for processing their personal data, how it uses such data and the legal basis for processing in its privacy notices. It will not process personal data of individuals for other reasons.

Where the organisation processes special categories of personal data or criminal records data to perform obligations or to exercise rights in employment law, this is done in accordance with particular guidance on special categories of data and criminal records data.

The organisation will update personal data promptly if an individual advises that his/her information has changed or is inaccurate.

Personal data gathered is held both electronically and in hard copy formats, although the majority of data is now held electronically. The periods for which the organisation holds personal data are contained in its privacy notices to individuals.

## Individual rights

As a data subject, individuals have a number of rights in relation to their personal data.

### *Subject access requests*

Individuals have the right to make a subject access request. If an individual makes a subject access request, the Co-operative College will tell him/her:

- whether or not his/her data is processed and if so why, the categories of personal data concerned and the source of the data if it is not collected from the individual;
- to whom his/her data is or may be disclosed, including to recipients located outside the European Economic Area (EEA) and the safeguards that apply to such transfers;
- for how long his/her personal data is stored (or how that period is decided);
- his/her rights to rectification or erasure of data, or to restrict or object to processing;

- his/her right to complain to the Information Commissioner if he/she thinks the organisation has failed to comply with his/her data protection rights; and
- whether or not the College carries out automated decision-making and the logic involved in any such decision-making.

The Co-operative College will also provide the individual with a copy of the personal data undergoing processing. This will normally be in electronic form if the individual has made a request electronically, unless he/she agrees otherwise.

To make a subject access request, the individual should send the request to data@co-op.ac.uk . In some cases, the College may need to ask for proof of identification before the request can be processed. The Co-operative College will inform the individual if it needs to verify his/her identity and the documents it requires.

The Co-operative College will normally respond to a request within a period of one month from the date it is received. In some cases, such as where the College processes large amounts of the individual's data, it may respond within three months of the date the request is received. The College will write to the individual within one month of receiving the original request to tell him/her if this is the case.

If a subject access request is manifestly unfounded or excessive, the College is not obliged to comply with it. Alternatively, the College can agree to respond but will charge a fee, which will be based on the administrative cost of responding to the request. A subject access request is likely to be manifestly unfounded or excessive where it repeats a request to which the organisation has already responded. If an individual submits a request that is unfounded or excessive, the College will notify him/her that this is the case and whether or not it will respond to it.

***Other rights***

Individuals have a number of other rights in relation to their personal data. They can require the College to:

- rectify inaccurate data;
- stop processing or erase data that is no longer necessary for the purposes of processing;
- stop processing or erase data if the individual's interests override the College's legitimate grounds for processing data (where the College relies on its legitimate interests as a reason for processing data);
- stop processing or erase data if processing is unlawful; and
- stop processing data for a period if data is inaccurate or if there is a dispute about whether or not the individual's interests override the College's legitimate grounds for processing data.

To ask the organisation to take any of these steps, the individual should send the request to data@co-op.ac.uk

## Data security

The Co-operative College takes the security of personal data seriously. The College has internal policies and controls in place to protect personal data against loss, accidental destruction, misuse or disclosure, and to ensure that data is not

accessed, except by employees in the proper performance of their duties. Please refer to the College's IT and Computer Use Policy for further details on data security.

Where the organisation engages third parties to process personal data on its behalf, such parties do so on the basis of written instructions (in the form of a contract between the two parties), are under a duty of confidentiality and are obliged to implement appropriate technical and organisational measures to ensure the security of data.

## Data Breaches

If the Co-operative College discovers that there has been a breach of personal data that poses a risk to the rights and freedoms of individuals, it will report it to the Information Commissioner within 72 hours of discovery. The College will record all data breaches regardless of their effect.

If the breach is likely to result in a high risk to the rights and freedoms of individuals, it will tell affected individuals that there has been a breach and provide them with information about its likely consequences and the mitigation measures it has taken.

## International data transfers

Personal data will only be transferred to countries outside the EEA in order to facilitate or accommodate international delivery of the College's services or products. For example, in applying for visas, booking accommodation, etc.

We will transfer the personal information we collect about you to the USA outside the EU for processing and storage. This is because the systems we use (Google and Salesforce) are international products and these companies process and store data in the USA. There is an adequacy decision by the European Commission in respect of the USA. This means that the country to which we transfer your data is deemed to provide an adequate level of protection for your personal information. To ensure your personal information receives an adequate level of protection we have put in place the following appropriate measure to ensure your personal information is treated by those third parties in a way that is consistent with and which respects the EU and UK laws on data protection. Organisations processing data in the USA are certified under the Privacy Shield Framework. Further information about protective measures can be requested from the College's IT provider – Co-operatives UK.

## Individual responsibilities – Staff and Associates

Individuals are responsible for helping the College keep their personal data up to date. Individuals should let the College know if data provided to the College changes, for example if an individual moves house or changes his/her email address.

Individuals may have access to the personal data of other individuals including our members, customers and clients in the course of their employment or working contract. Where this is the case, the organisation relies on individuals to help meet its data protection obligations to staff and to members, customers and clients.

Individuals who have access to personal data are required:

- to access only data that they have authority to access and only for authorised purposes;
- not to disclose data except to individuals (whether inside or outside the organisation) who have appropriate authorisation;
- to keep data secure (for example by complying with rules on access to premises, computer access, including password protection, and secure file storage and destruction);
- not to remove personal data, or devices containing or that can be used to access personal data, from the organisation's premises without adopting appropriate security measures (such as encryption or password protection) to secure the data and the device; and
- not to store personal data on local drives or on personal devices that are used for work purposes.

Further details about the College's security procedures can be found in its IT and Computer Use Policy.

Failing to observe these requirements may amount to a disciplinary offence, which will be dealt with under the College's disciplinary procedure. Significant or deliberate breaches of this policy, such as accessing personal data without authorisation or a legitimate reason to do so, may constitute gross misconduct and could lead to dismissal without notice.

## Publication of College Information

Information that is already in the public domain is exempt from the regulations. It is College policy to make as much information public as possible, and in particular the following information will be available to the public:

- Names of Board of Trustee members, details of application to become a board member and register of interests.
- Names and positions of senior post holders and register of interests.

Any individual who has good reason for wishing details to remain confidential should contact the Learning Technologist at data@co-op.ac.uk

## Retention of Data

Personal data will be retained for no longer than is necessary for the purpose for which it was collected. Standard retention times are necessary to meet various contractual requirements.

A full set of employment data (contained within personnel files) will be kept for the duration of employment and for a period of 5 years from the end of employment. A summary of the employee's record of service (for the purpose of providing employment references) will be retained for a period of 10 years from the end of employment.

Member data will be retained for the duration of membership and for a period of 3 years after which membership has ceased.

Standard retention times for finance related documents are specified in the College Finance Regulations.

## Disposal of Data

Particular care must be taken with the disposal of personal data. Staff should be aware that the same standards should be applied to informal records, lists and printouts held by individual members of staff containing personal data as to records which are part of the formal College records system.

This material must not be disposed of in ordinary office waste paper bins.

Personal data must be destroyed by secure methods such as shredding.

Information stored on obsolete electronic equipment (desktops, laptops and other devices) will be erased prior to them being sold or disposed of.

## Direct Marketing

The College will only use personal data for promotional campaigns or to market additional activities where the individual has given consent. Any staff wishing to send out marketing material must check with the Marketing & Communications Manager to verify consent.

## Use of Photographs

Where practicable, the Co-operative College will seek consent from individuals before displaying photographs in which they appear. If this is not possible (for example, a large group photo), the College will remove any photograph if a complaint is received. This policy also applies to photographs published on the organisations website, newsletters or any social networking sites.