Westminster College
A resource centre for learning
Serving the United Reformed Church

Policy and procedure Manual

Data Protection Policy

040T. "Staff" Revised March 2018 to be revised March 2021

1. Who the policy applies to

This policy applies to all "staff" providing services to Westminster College, including teaching, assessment, archiving and governing.

2. Why the policy is needed

Westminster College is committed to a policy of protecting the rights and privacy of its employees, students, former students and other users, defined as "data subjects" in accordance with the General Data Protection Regulations (GDPR). Westminster College needs to process "personal data", as it is often referred to, according to the principles contained within the regulation.

Westminster staff has a personal responsibility to ensure that they adhere to Westminster College's Data Protection Policy and the Regulation.

Any breach of this Policy, or the Regulation, can be considered as a disciplinary matter. It may also be a criminal matter for which Westminster College, and the individual concerned, could be held criminally liable.

3. The policy principles

Policy Statement

To comply with the eight Data Protection Principles, these define how data can be legally processed. "Processing" includes obtaining, recording, holding or storing information and using it in any way. The information about individuals must be collected and used fairly, stored safely and securely and not disclosed unlawfully to any third party (without the express consent of the individual).

Article 5 of the GDPR requires that personal data must:

1. **Be processed lawfully, fairly and only when certain conditions are met**;
2. **Only be collected and processed for specified and lawful purposes**;
3. **Be adequate, relevant and not excessive;**
4. **Be accurate and, where necessary, kept up to date**;
5. **Be kept for no longer than necessary;**
6. **Be processed in accordance with data subjects' right**
7. **Be protected by appropriate security measures;**
8. **Not transferred outside the European Economic Area, to countries without adequate protection unless the consent of the data subject has been obtained.**

The Regulation defines both personal data and special personal data (refer to definitions in Section 4). Data users must ensure that the necessary conditions are satisfied for the

processing of personal data. In addition, they must adhere to the extra, more stringent conditions in place for the processing of special personal data. Special personal data should normally only be processed if the data subjects have given their explicit (written) consent to this processing, and must be protected with a higher level of security. It is recommended that special records are kept separately in a locked drawer or filing cabinet, or in a password-protected computer file. (We note that information about religious beliefs is special data).

Security

The security of personal data in the possession of Westminster College is of paramount importance and is, therefore, addressed in various policies and procedures.
Westminster College security procedures include:

- Entry controls to prevent unauthorised people gaining access to confidential information and personal data.
- Lockable desks and cupboards for secure storage of confidential information and personal data.
- Shredding for paper records with confidential information and personal data that is no longer being stored.
- Ensuring unauthorised people are not able to see confidential information on paperwork or computer screens being used by staff.
- Laptops or notebooks should use pseudonymisation and encryption.

Use of personal data

Use of personal data must be only in accordance with Westminster College data protection policy and privacy notices. If other uses are required the relevant privacy notice must first be updated and the data subjects covered by the notice informed.

Responsibilities – General Principle

All personal data held on behalf of Westminster College, whether electronically or on paper, must be kept securely, no matter whether it is kept by an individual or on the commonly-accessible server. Personal data must not be disclosed to any unauthorised third party by any means, accidentally or otherwise.

Where staff is unsure as to whether they can legitimately share/disclose personal data with other individuals, either within or outside Westminster College, they must seek advice from their manager.

All staff should note that unauthorised disclosure may be a disciplinary matter. It may also be a criminal matter for which Westminster College and the individual concerned could be held criminally liable.

Board of Governors Responsibilities

- All staff are aware of their responsibilities under the Data Protection Policy and the Regulations and of the risks/consequences of failure to comply with the related requirements.
- That mechanisms are put in place to protect data (and particularly special data) during day-to- day operations.

- All personal data being processed within Westminster College complies with the Data Protection Policy (including any subsequent amendments or additions) and with the Regulations.
- That all forms and correspondence used by Westminster College to request personal data clearly state the purposes for which the information is to be used, the period of time it is to retained, and to whom it is likely to be disclosed.
- All personal data held within Westminster College is kept securely and is disposed of in a safe and secure manner when no longer needed.
- All Data Protection breaches are notified to the Chair of the Governing body, with remedial action taken to mitigate the risk of reoccurrence.
- An annual audit of the personal data within Westminster College is carried out and recorded.
- Where a new or different purpose for processing data is introduced, the policy and/or privacy notices are updated.
- Westminster College's Data Protection Policy is regularly reviewed and updated in line with best practice.
- Staff has access to training on their responsibilities under the Data Protection Policy and the Regulation, both on-line and through more traditional training methods.
- Responses to requests for information under the Regulation, and related compliance matters, are dealt with in a timely manner and in line with the requirements of the Regulation.
- Advice and guidance on any area of the Policy or the Regulation is provided to staff and students, on request.

Staff Responsibilities

All staff must take personal responsibility for ensuring that:

- They are aware of their responsibilities under the Data Protection Policy and the Regulation and the risks/consequences of failure to comply with the related requirements. Where they are uncertain of their responsibilities, they must raise this with their manager.
- They complete on-line training if they require further information about data security.
- Personal data relating to any living individual (staff, trustees, students, contractors, members of the public etc.) which they hold or process is kept securely.
- Personal data relating to any living individual is not disclosed, either orally or in writing, accidentally or otherwise, to any unauthorised third party.
- All Data Protection breaches are notified to their manager, with remedial actions implemented to mitigate the risk of reoccurrence.
- When supervising students who are processing personal data, that they are aware of this policy.
- Personal data which they provide in connection with their employment is accurate and up-to-date, and that they inform Westminster College of any errors, corrections or changes, for example, change of address.

- Passers-by cannot read confidential information from papers or computer monitors; this includes locking computers when left unattended.
- Never giving out personal information by telephone without being confident that the caller is entitled to it; requests by email should be encouraged

Student Responsibilities

All students must take personal responsibility for ensuring that:

- When using Westminster College's facilities to process personal data (for example, in course work or research), they seek advice from their Tutor on their responsibilities under the Regulation.
- Personal data which they provide in connection with their studies is accurate and up-to-date, and that they inform Westminster College of any errors, corrections or changes, for example, change of address.

Disposal Policy for Personal Data

The Regulation places an obligation on Westminster College to exercise care in the disposal of personal data, including protecting its security and confidentiality during storage, transportation, handling, and destruction.

All staff have a responsibility to consider safety and security when disposing of personal data in the course of their work. Consideration should also be given to the nature of the personal data involved, how sensitive it is, and the format in which it is held.

Retention Policy for Personal Data Records

The Regulation places an obligation on Westminster College not to hold personal data for longer than is necessary. Westminster College's policy is to use the retention periods suggested in the University of Cambridge's Master Records Retention Schedule, as updated from time to time, see www.information-compliance.admin.cam.ac.uk/records-management.

Contractors, Short-Term and Voluntary Staff

Westminster College is responsible for the use made of personal data by anyone working on its behalf, whether as an agent, in a voluntary capacity, or as a consultant or contractor undertaking work for Westminster College.

Transfer of Data Outside Westminster College

When Westminster College shares personal data with another organisation, liability for adherence to the Regulation, in relation to this data, rests with Westminster College. Should the receiving organisation breach the Regulation, Westminster College would be held responsible for that breach.

A data sharing agreement may be required before sharing personal data with other organisations in order to conduct business.

Transfer of Data Overseas

The Eighth Data Protection Principle prohibits the transfer of personal data to any country outside the European Economic Area (EEA) (EU Member States, Iceland, Liechtenstein and Norway) unless that country ensures an adequate level of protection for data subjects.

In all instances where personal data is being sent outside the EEA, the consent of the data subject should be obtained before their personal information is sent. This includes

requests for personal data including from overseas colleges, financial sponsors and foreign governments.

Privacy notices

Privacy notices are provided on the website that should be read in conjunction with this policy.

Use of images

Westminster College will gain the consent of individuals whose images are used for marketing and PR activities, including in-print, online and on social media. We acknowledge that restrictions can be put on staff using such images in their personal publishing but that other people are outside the college's control.

Data Protection Officer

Westminster College does not have (and is not required to have) an appointed Data Protection Officer, but has a Data Protection Lead, currently the Bursar.

Making a Request

Staff, students, users of Westminster College's facilities, and members of the public have the right to access personal data that is being kept about them insofar as it falls within the scope of the Regulation. Requests should be made in writing via email to gdpr@westminster.cam.ac.uk or by post to Westminster College, Madingley Road, Cambridge, CB3 0AA.

Westminster College does not charge for the first request an administrative fee to access information and will seek to ensure that the information is provided within 30 calendar days.

There is no right to an internal review of a decision taken regarding release of personal information. If the requestor is not satisfied with the response received from Westminster College, they do, however, have the right to appeal directly to the e Information Commissioner's Office at Wycliffe House, Water Lane, Wilmslow, SK9 5AF (ico.org.uk).

4. The definition of terms used in the document

Definitions

- **'Data Controller'**: A natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.
- **'Data Subject'**: any individual who is the subject of personal data held by an organisation, excluding deceased individuals or/and individuals who cannot be identified or distinguished from others (i.e. employees, customers and consumers)
- **'Personal Data'**: any **information** relating to an identified or **identifiable natural person** ('data subject'); an identifiable natural person is one who can be identified, **directly** or **indirectly,** in particular by reference to an identifier such as **name,** an **identification number, location data, an online identifier** or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
- **'Special Personal Data'** : different from ordinary personal data (see above) and relates to racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, physical or mental health or condition, sex life or sexual orientation, genetic and biometric data.

- **'Processing'**: in relation to information or data it means obtaining, recording or holding the information or data, or carrying out any operation or set of operations on the information or data, this covers nearly everything from the storage, access, retrieval, disclosure and erasure/destruction of data in any form.
- **'Third Party'**: any individual/organisation other than the data subject and the data controller (Westminster College).

5. How the policy will be applied

The Human Rights Act states that everyone has the right to respect for their private and family life, their home and their correspondence. However, it may be acceptable to override this right if it is in accordance with the law and for the reasons given below under "Disclosure of Data".

What right do I have to access of information?

- Under the rules of GDPR, individuals are allowed to view certain information held about them.
- In relation to references, medical records and disciplinary records, employees can request to see the information that is kept on them.
- Westminster College will use its discretion to disclose information as far as it is reasonably practicable to do so. In certain circumstances, in order to protect the rights of a third party, it may not be appropriate to do so.

6. Responsibility for administering and updating the policy

The Bursar is responsible for updating this policy in consultation with the Principal, the Convenors of Management Committee and the Governing Body; and also actively seeking advice from United Reformed Church Human Relations Department as necessary.

7. When it was last revised, when it will next be revised.

May 2018
May 2020

8. The date from which it applies

25th May 2018

9. Statutory regulations and good practice guidance

General Data Protection Regulations

It applies uniformly across EU member states, it is technologically neutral. The purpose of GDPR is for the regulation of the processing of information relating to individuals; to make provision in connection with the Information Commissioner's functions under certain regulations relating to information, to make provision for a direct marketing code of conduct; and for connected purposes.

Human Rights Act 1998

10. Further Information

Information Commissioner's Webpage - http://www.ico.gov.uk/
ACAS - http://www.acas.co.uk/