Wesley House data protection policy

Introduction

Wesley House, Cambridge is committed to protecting the rights and privacy of individuals in accordance with the Data Protection Act 1998 ("the Act") and, from May 2018, the EU General Data Protection Regulation. This document is the College's policy in response to the requirements of the Act.

Purpose and Scope

In carrying out its responsibilities, the College is required to process certain information about individuals such as staff, students, former students and other users, defined as "data subjects" in the Act. This information, or "personal data" as it is often referred to, must be processed according to the principles contained within the Act.

Wesley House staff and Trustees, or others who process or use any personal information on behalf of the College (i.e. "data users"), have a personal responsibility to ensure that they adhere to the College's Data Protection Policy and the Act.

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

Data Protection Principles

Wesley House data users must 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.

Personal data must:

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

The Act defines both personal data and sensitive personal data (please refer to the Definitions section below). 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 sensitive personal data. Sensitive 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 sensitive records are kept separately in a locked drawer or filing cabinet, or in a password-protected computer file.

Security

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

The College's 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.

Use of personal data

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

Responsibilities - General Principles

All personal data held on behalf of the 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 are unsure as to whether they can legitimately share/disclose personal data with other individuals, either within or outside the College, they must seek advice from their line manager.

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

Trustee Responsibilities

Trustees have responsibility for ensuring that:

- All staff are aware of their responsibilities under the Data Protection Policy and the Act and of the risks/consequences of failure to comply with the related requirements.
- That mechanisms are put in place to protect data (and particularly sensitive data) during day-to- day operations.
- All personal data being processed within the College complies with the Data Protection Policy (including any subsequent amendments or additions) and with the Act.
- That all forms and correspondence used by the 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 the 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 Trustees, with remedial action taken to mitigate the risk of reoccurrence.
- An annual audit of the personal data within the 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.
- The College's Data Protection Policy is regularly reviewed and updated in line with best practice.
- Staff have access to training on their responsibilities under the Data Protection Policy and the Act, both on-line and through more traditional training methods.
- Responses to requests for information under the Act, and related compliance matters, are dealt with in a timely manner and in line with the requirements of the Act.
- Advice and guidance on any area of the Policy or the Act 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 Act 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 line 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 line 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 the College of any errors, corrections or changes, for example, change of address.
- Passers-by can not 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 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 Act.
- Personal data which they provide in connection with their studies is accurate and up-to-date, and that they inform the College of any errors, corrections or changes, for example, change of address.

Disposal Policy for Personal Data

The Act places an obligation on the 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.

The College has a contract with a secure shredding service for the disposal of confidential information.

Retention Policy for Personal Data Records

The Act places an obligation on the College not to hold personal data for longer than is necessary. Wesley House'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.

Contractors, Short-Term and Voluntary Staff

The 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 the College.

Transfer of Data Outside the College

When the College shares personal data with another organisation, liability for adherence to the Act, in relation to this data, rests with Wesley House. Should the receiving organisation breach the Act, Wesley House 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.

Use of CCTV

The College's use of CCTV is governed by a Code of Practice, issued by the ICO: https://ico.org.uk/media/for-organisations/documents/1542/cctv-code-of-practice.pdf

For reasons of crime prevention and security a network of surveillance cameras is in operation throughout the College. The presence of these cameras may not be obvious. This policy determines that personal data obtained during monitoring will be processed as follows:

- The recordings will be accessed only by College staff, Trustees and the Lay Chaplain;
- Personal data obtained during monitoring will be destroyed as soon as possible after any investigation is complete;
- Staff involved in monitoring will maintain confidentiality in respect of personal data.

Privacy notices

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

Use of images

Wesley House will gain the consent of individuals whose images are used for the college's 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

The Data Protection Officer for Wesley House is the Business Director.

Making a Request

Staff, students, users of the 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 Act. Requests should be made in writing via email to office@wesley.cam.ac.uk or via post to: Wesley House, Jesus Lane, Cambridge, CB5 8BJ

The College does not charge 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 the College they do, however, have the right to appeal directly to the ICO.

Definitions

Data	Information which is being used or held in a computerised system, or a 'relevant filing system' i.e. a manual filing system that is structured in such a way that data contained within it is readily accessible. Data can be written information, photographs, fingerprints or voice recordings.
Personal Data	Information that identifies and relates to a living individual, and includes any expression of opinion or intention about the individual.
Sensitive Personal Data	Personal data consisting of information as to race/ethnic origin; political opinion; religious or similar beliefs; trade union membership; physical or mental health or condition; sexual life; and criminal record.
Processing	Anything which can be done with personal data i.e. obtaining, recording, holding, organising, adapting, altering, retrieving, consulting, disclosing, aligning, combining, blocking, erasing, destroying etc.
Data Subject	An individual who is the subject of personal data. This will include: staff, current and prospective students, graduates, suppliers of goods and services, business associates, conference delegates, survey respondents etc.
Data Controller	Refers to Wesley House, Cambridge. This includes College staff who collect and process data on behalf of the College, and students who are collecting and processing personal data or as part of their studies.
Data Processor	Any person (other than an employee of the College) who processes personal data on behalf of the College e.g. printing agency.
Data Users	Refers to both Data Controller and Data Processors.