Waltham Forest College

Data Protection Policy
GDPR

This document can be made available in other formats, on request

Date of Publication	**31 July 2019**
Date of Review	**Approval date + 1 year**
Line Manager Responsible	**Dr Joy Kettyle**
Policy Creator	**Corporation Audit Committee**
Approved by the Corporation	
Version control	**5**

Rationale

Waltham Forest College (WFC) is committed to a policy of protecting the rights and privacy of individuals, including learners, staff and others, in accordance with the General Data Protection Regulation (GDPR) May 2018.

The new regulatory environment demands higher transparency and accountability in how colleges manage and use personal data. It also accords new and stronger rights for individuals to understand and control that use.

The GDPR contains provisions that the college will need to be aware of as data controllers, including provisions intended to enhance the protection of student's personal data. For example, the GDPR requires that we must ensure that our college privacy notices are written in a clear, plain way that staff and students will understand.

WFC needs to process certain information about its staff, students, parents and guardians and other individuals with whom it has a relationship for various purposes such as, but not limited to:

1. The recruitment and payment of staff.
2. The administration of programmes of study and courses.
3. Student enrolment.
4. Examinations and external accreditation.
5. Recording student progress, attendance and conduct.
6. Collecting fees.
7. Complying with legal obligations to funding bodies and government including local government.
8. If you opted in for marketing in the future with regards to new course offerings we will only contact you on your preferred method with details of new courses or news from Waltham Forest College such as a newsletter

To comply with various legal obligations, including the obligations imposed on it by the General Data Protection Regulation (GDPR) WFC will ensure that all this information about individuals is collected and used fairly, stored safely and securely, and not disclosed to any third party unlawfully.

Compliance

This policy applies to all staff and students of WFC. Any breach of this policy or of the Regulation itself will be considered an offence and the college's disciplinary procedures will be invoked.

As a matter of best practice, other agencies and individuals working with WFC and who have access to personal information, will be required to read and comply with this policy. It is expected that departments who are responsible for dealing with external bodies will take the responsibility for ensuring that such bodies sign a contract which among other things will include an agreement to abide by this policy.

This policy will be updated as necessary to reflect best practice in data management, security and control and to ensure compliance with any changes or amendments to the GDPR and other relevant legislation. The Code of Practice on GDPR for WFC gives further detailed guidance and WFC undertakes to adopt and comply with this Code of Practice.

General Data Protection Regulation (GDPR)

This piece of legislation comes in to force on the 25 May 2018. The GDPR regulates the processing of personal data, and protects the rights and privacy of all living individuals (including children), for example by giving all individuals who are the subject of personal data a general right of access to the personal data which relates to them. Individuals can exercise the right to gain access to their information by means of a 'subject access request'. Personal data is information relating to an individual and may be in hard or soft copy (paper/manual files; electronic records; photographs; CCTV images), and may include facts or opinions about a person.

The GDPR also sets out specific rights for college students in relation to educational records held within the state education system. These rights are set out in separate education regulations 'The Education (Pupil Information) (England) Regulations 2000'. For more detailed information on these Regulations see the Data Protection Data Sharing Code of Practice (DPCoP) from the Information Commissioner's Office (ICO). Please follow this link to the ICO's website (www.ico.gov.uk)

Responsibilities under the GDPR

WFC will be the 'data controller' under the terms of the legislation – this means it is ultimately responsible for controlling the use and processing of the personal data. The college appoints a Data Protection Officer (DPO), currently Kalim Uddin who is available to address any concerns regarding the data held by college and how it is processed, held and used. WFC has nominated the Audit Committee to oversee this policy.

The Executive Team is responsible for all day-to-day data protection matters, and it will be responsible for ensuring that all members of staff and relevant individuals abide by this policy, and for developing and encouraging good information handling within the college.

The Executive Team is also responsible for ensuring that the college's notification is kept accurate. Details of the college's notification can be found on the Office of the Information Commissioner's website. Our data registration number is: Z8743455

Compliance with the legislation is the personal responsibility of all members of the college who process personal information.

Individuals who provide personal data to the college are responsible for ensuring that the information is accurate and up-to-date.

Data Protection Principles

The legislation places a responsibility on every data controller to process any personal data in accordance with the eight principles. More detailed guidance on how to comply with these principles can be found in the Data Protection Data Sharing Code of Practice (DPCoP). Please follow this link to the ICO's website (www.ico.gov.uk)

In order to comply with its obligations, WFC undertakes to adhere to the eight principles:

1) Process personal data fairly and lawfully.

WFC will make all reasonable efforts to ensure that individuals who are the focus of the personal data (data subjects) are informed of the identity of the data controller, the purposes of the processing, any disclosures to third parties that are envisaged; given an indication of the period for which the data will be kept, and any other information which may be relevant. For example,

2) Process the data for the specific and lawful purpose for which it collected that data and not further process the data in a manner incompatible with this purpose.

WFC will ensure that the reason for which it collected the data originally is the only reason for which it processes those data, unless the individual is informed of any additional processing before it takes place.

3) Ensure that the data is adequate, relevant and not excessive in relation to the purpose for which it is processed.

WFC will not seek to collect any personal data which is not strictly necessary for the purpose for which it was obtained. Forms for collecting data will always be drafted with this mind. If any irrelevant data are given by individuals, they will be destroyed immediately.

4) Keep personal data accurate and where necessary, up to date.

WFC will review and update all data on a regular basis. It is the responsibility of the individuals giving their personal data to ensure that this is accurate, and each individual should notify the college if, for example, a change in circumstances mean that the data needs to be updated. It is the responsibility of the college to ensure that any notification regarding the change is noted and acted on.

5) Only keep personal data for as long as is necessary.

WFC undertakes not to retain personal data for longer than is necessary to ensure compliance with the legislation, and any other statutory requirements. This means WFC will undertake a regular review of the information held and implement a weeding process. WFC will dispose of any personal data in a way that protects the rights and privacy of the individual concerned (e.g. secure electronic deletion, shredding and disposal of hard copy files as confidential waste). A log will be kept of the records destroyed.

6) Process personal data in accordance with the rights of the data subject under the legislation.

Individuals have various rights under the legislation including a right to:

- Be told the nature of the information the college holds and any parties to whom this may be disclosed.
- Prevent processing likely to cause damage or distress.
- Prevent processing for purposes of direct marketing.
- Be informed about the mechanics of any automated decision making process that will significantly affect them.
- Not have significant decisions that will affect them taken solely by automated process.
- Sue for compensation if they suffer damage by any contravention of the legislation.
- Take action to rectify, block, erase or destroy inaccurate data.
- Request that the Office of the Information Commissioner assess whether any provision of the Act has been contravened.

WFC will only process personal data in accordance with individuals' rights.

7) Put appropriate technical and organisational measures in place against unauthorised or unlawful processing of personal data, and against accidental loss or destruction of data.

All members of staff are responsible for ensuring that any personal data which they hold is kept securely and not disclosed to any unauthorised third parties. WFC will ensure that all personal data is accessible only to those who have a valid reason for using it.

WFC will have in place appropriate security measures e.g. ensuring that hard copy personal data is kept in lockable filing cabinets/cupboards with controlled access (with the keys then held securely in a key cabinet with controlled access):

- Keeping all personal data in a lockable cabinet with key-controlled access.
- Password protecting personal data held electronically.
- Archiving personal data which are then kept securely (lockable cabinet).
- Placing any PCs or terminals, CCTV camera screens etc. that show personal data so that they are not visible except to authorised staff.
- Ensuring that PC screens are not left unattended without a password protected screen-saver being used.

In addition, WFC will put in place appropriate measures for the deletion of personal data - manual records will be shredded or disposed of as 'confidential waste' and appropriate contract terms will be put in place with any third parties undertaking this work. Hard drives of redundant PCs will be wiped clean before disposal or if that is not possible, destroyed physically. A log will be kept of the records destroyed.

This policy also applies to staff and students who process personal data 'off-site', e.g. when working at home, and in circumstances additional care must be taken regarding the security of the data.

8) Ensure that no personal data is transferred to a country or a territory outside the European Economic Area (EEA) unless that country or territory ensures adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

WFC will not transfer data to such territories without the explicit consent of the individual.

This also applies to publishing information on the internet - because transfer of data can include placing data on a website that can be accessed from outside the EEA - so WFC will always seek the consent of individuals before placing any personal data (including photographs) on its website.

If the college collects personal data in any form via its website, it will provide a clear and detailed privacy statement prominently on the website, and wherever else personal data is collected.

Our legal basis for processing for the personal data:

• If you decided to enter into a learner agreement with Waltham Forest College under the contract we will need to process your details as defined by legislation.

Consent as a basis for processing

Although it is not always necessary to gain consent from individuals before processing their data, it is often the best way to ensure that data is collected and processed in an open and transparent manner.

Consent is especially important when WFC is processing any sensitive data, as defined by the legislation. WFC understands consent to mean that the individual has been fully informed of the intended processing and has signified their agreement (e.g. via the enrolment form) whilst being of a sound mind and without having any undue influence exerted upon them. Consent obtained on the basis of misleading information will not be a valid basis for processing. Consent cannot be inferred from the non-response to a communication.

"Personal Details

- *For the purposes of the General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679 you consent to the college holding and processing personal data including sensitive personal data of which you are the subject, details of which are specified in the college's data protection policy.*
- *This will include marketing images and the college CCTV."*

WFC will ensure that any forms used to gather data on an individual will contain a statement (fair collection statement) explaining the use of that data, how the data may be disclosed and also indicate whether or not the individual needs to consent to the processing.

WFC will include the specified statement from the Department for Education (DfE) on the student enrolment form and update when required following the ESFA's technical guidance:

How We Use Your Personal Information

This privacy notice is issued by the Education and Skills Funding Agency (ESFA), on behalf of the Secretary of State for the DfE. It is to inform learners how their personal information will be used by the DfE, the ESFA (an executive agency of the DfE) and any successor bodies to these organisations. For the purposes of the Data Protection Act 1998, the DfE is the data controller for personal data processed by the ESFA. Your

personal information is used by the DfE to exercise its functions and to meet its statutory responsibilities, including under the Apprenticeships, Skills, Children and Learning Act 2009 and to create and maintain a unique learner number (ULN) and a personal learning record (PLR). Your information may be shared with third parties for education, training, employment and well-being related purposes, including for research. This will only take place where the law allows it and the sharing is in compliance with the Data Protection Act 1998. The English European Social Fund (ESF) Managing Authority (or agents acting on its behalf) may contact you in order for them to carry out research and evaluation to inform the effectiveness of training.
You can opt out of contact for other purposes by ticking any of the following boxes if you do not wish to be contacted:

- *About courses or learning opportunities.*
- *For surveys and research.*
- *By post.*
- *By phone.*
- *By email.*

Further information about use of and access to your personal data, and details of organisations with whom we regularly share data are available at:

https://www.gov.uk/government/publications/esfa-privacy-notice

WFC will ensure that if the individual does not give his/her consent for the processing, and there is no other lawful basis on which to process the data, then steps will be taken to ensure that processing of that data does not take place.

Retention period
The Waltham Forest College will process personal data for the length of any agreement we have in place to manage a course we provide. If we cannot or you choose not to take out a course we provide you with we will destroy your details unless you have opted in for further contact in regards to new courses or news from Waltham Forest College. We will always provide you with the opportunity to opt out on all future correspondence such as email opt out.

Subject Access Rights (SARs)

Individuals have a right to access any personal data relating to them which are held by the college. Any individual wishing to exercise this right should apply in writing to the Principal. Any member of staff receiving a Subject Access Request should forward this to the Principal. Under the terms of the legislation, any such requests must be complied with within 40 days. For detailed guidance on responding to Subject Access Requests, see the Code of Practice (CoP).

Disclosure of Data

Only disclosures which have been notified under the college's Data Protection notification must be made and therefore staff and students should exercise caution when asked to disclose personal data held on another individual or third party.

Enforcements & Breaches

Any loss of data must be reported to the Data Protection Officer (DPO) for an assessment of the risks associated with the breach.

In addition, if special or personal data about a student or member of staff is either inadvertently released or used inappropriately, the DPO is to be informed as soon as the breach is discovered so that appropriate action can be taken.
The DPO is responsible for:

- informing appropriate people and organisations that the breach has occurred;
- notifying serious breaches (based on current ICO guidance);
- implementing a recovery plan, including damage limitation; and
- reviewing and updating information security.

Linked policies, procedures and guidance

- For further information and guidance, please see:
- Student Acceptable use Statement
- Staff Acceptable use Statement
- Data Retention Schedule
- Information Security Policy

To find out more about the General Data Protection Regulation please visit www.ico.org.uk

WFC undertakes not to disclose personal data to unauthorised third parties, including family members, friends, government bodies and in some circumstances, the police.

Legitimate disclosures may occur in the following instances:

- the individual has given their consent to the disclosure.
- the disclosure has been notified to the Office of Information Commissioner (OIC) and is in the legitimate interests of the college.
- the disclosure is required for the performance of a contract.

There are other instances when the legislation permits disclosure without the consent of the individual. For detailed guidance on disclosures see the Code of Practice.

In no circumstances will WFC sell any of its databases to a third party.

Publication of College Information

WFC publishes various items which will include some personal data, e.g.

- internal telephone directory.
- event information.
- photos and information in marketing materials.

It may be that in some circumstances an individual wishes their data processed for such reasons to be kept confidential, or restricted college access only. Therefore it is WFC policy to offer an opportunity to opt-out of the publication of such when collecting the information.

Email
It is the policy of WFC to ensure that senders and recipients of email are made aware that under the DPA, and Freedom of Information Legislation, the contents of email may have to be disclosed in response to a request for information. One means by which this will be communicated will be by a disclaimer on the college's email. Under the Regulation of Investigatory Powers Act 2000, Lawful Business Practice Regulations, any email sent to or from the college may be accessed by someone other than the recipient for system management and security purposes.

CCTV
There are some CCTV systems operating within WFC for the purpose of protecting college members and property. WFC will only process personal data obtained by the CCTV system in a manner which ensures compliance with the legislation.

Procedure for review

This policy will be updated as necessary to reflect best practice or future amendments made to the General Data Protection Regulation (GDPR) May 2018 and Data Protection Act 1998.

Please follow this link to the ICO's website (www.ico.gov.uk) which provides further detailed guidance on a range of topics including individuals' rights, exemptions from the Act, dealing with subject access requests, how to handle requests from third parties for personal data to be disclosed etc. In particular, you may find it helpful to read the Guide to Data Protection which is available from the website.

For help or advice on any data protection, please do not hesitate to contact:

The Data Protection Officer (DPO):
Waltham Forest College
Forest Road
London E17 4JB
dpo@waltham.ac.uk

For further information, please read our student, staff and visitor privacy statements, including our data retention schedule on our website.

Glossary of Terms

Personal Data - "Personal data" means any information relating to an identified or identifiable natural person ("data subject"); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data**,** online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.

Sensitive Personal Data - "Sensitive Personal Data" are personal data, revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership; data concerning health or sex life and sexual orientation; genetic data or biometric data**.** Data relating to criminal offences and convictions are addressed separately (as criminal law lies outside the EU's legislative competence).

Processing - "Processing" means any operation or set of operations performed upon personal data or sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Data Controller - "Controller" means the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by EU or Member State laws, the controller (or the criteria for nominating the controller) may be designated by those laws.

Data Processor - "Processor" means a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller.

Data Subject - a natural person whose personal data is processed by a controller or processor.

Data Protection Officer - an expert on data privacy who works independently to ensure that an entity is adhering to the policies and procedures set forth in the GDPR.

Recipient - entity to which the personal data are disclosed.

ICO- Information Commissioners Office UK statuary authority for Data Protection

Consent- "The consent of the data subject" means any freely given, specific, informed and unambiguous indication of his or her wishes by which the data subject, either by a statement or by a clear affirmative action**,** signifies agreement to personal data relating to them being processed.

Data Breaches - "Data breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

Biometric Data - any personal data relating to the physical, physiological, or behavioral characteristics of an individual which allows their unique identification.

Processing - any operation performed on personal data, whether or not by automated means, including collection, use, recording, etc.

Subject Access Right - also known as the Right to Access, it entitles the data subject to have access to and information about the personal data that a controller has concerning them.

Data Portability - the requirement for controllers to provide the data subject with a copy of his or her data in a format that allows for easy use with another controller.

Data Erasure - also known as the Right to be Forgotten, it entitles the data subject to have the data controller erase his/her personal data, cease further dissemination of the data, and potentially have third parties cease processing of the data.

Encrypted Data - personal data that is protected through technological measures to ensure that the data is only accessible/readable by those with specified access.