STAT05 - Data Protection Policy GDPR (General Data Protection Regulation)

Policy Author:	Clerk to the Corporation	**Policy Owner:**	Principal
Approval Date:	March 2022	**Review Date:**	October 2024

Purpose of the Policy

Weymouth College has a legal obligation to implement and adhere to the requirements of the **Data Protection Act 2018 as amended**

Please note changes resulting from Brexit:

- The EU's GDPR has been lifted into a new UK-GDPR (United Kingdom General Data Protection Regulation) that took effect on **January 31, 2020.**
- The Data Protection Act 2018 has been amended to be read in conjunction with the new UK-GDPR instead of the EU GDPR.
- An Adequacy Decision for the UK was adopted on **June 28, 2021** by the EU, securing unrestricted flow of personal data until June 2025.
- It is expected that the UK government will move to consolidate the two amended laws (UK-GDPR and Data Protection Act 2018) into one, comprehensive piece of data protection law at a later point.

Contents

1. Policy Statement

1.1. The College is committed to a policy of protecting the rights and privacy of individuals, including learners, staff and others.

1.2. 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. https://ico.org.uk/for-organisations/

2. Reason for the Policy

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

- The recruitment and payment of staff.
- The administration of programmes of study and courses.
- Student enrolment.
- Examinations and external accreditation.
- Recording student progress, attendance and conduct.
- Collecting fees.
- Complying with legal obligations to funding bodies and government including local government.

2.2. The UK GDPR contains provisions intended to enhance the protection of student's personal data. We must ensure that our college privacy notices are written in a clear, plain way that staff, students and service users will understand. https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/

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

2.4. The Data Protection Act 2018 (DPA) and the UK 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.

2.5. The Legislation also sets out specific rights for College students and service users 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). See the link below.

3. Data Protection Principles

The updated 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 Code of Practice. https://ico.org.uk/media/for-organisations/documents/1068/data_sharing_code_of_practice.pdf

1. **Process personal data fairly and lawfully.**
   Weymouth College 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.**
   Weymouth College 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 purposes for which it is processed**
   Weymouth College 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.**
   Weymouth College 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**
   Weymouth College undertakes not to retain personal data for longer than is necessary to ensure compliance with the legislation, and any other statutory requirements. This means Weymouth College will undertake a regular review of the information held and implement a weeding process.

   Weymouth College 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.

Weymouth College 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. Weymouth College will ensure that all personal data is accessible only to those who have a valid reason for using it.

- 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, Weymouth College 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, students and service users 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.

Weymouth College 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 Weymouth College 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.

4. Policy Objectives

4.1. This policy applies to all staff, students and service users of Weymouth College. Any breach of this policy or of the Regulation itself will be considered an offence and the College's disciplinary procedures will be invoked.

4.2. As a matter of best practice, other agencies and individuals working with Weymouth College and who have access to personal information, will be expected 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.

4.3. 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.

4.4. The Code of Practice on GDPR from the Information Commissioner's Office gives further detailed guidance and Weymouth College undertakes to adopt and comply with this Code of Practice.

5. Policy

The Data Controller and Data Protection Officers

5.1. Weymouth College is 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.

5.2. The appointed Data Protection Officers (DPO) are the Clerk to the Corporation and the Vice Principal Funding, Systems Development, and Operations who are available to address any concerns regarding the data held by college and how it is processed, held and used.

5.3. The Data Protection Officers are responsible for all day-to-day data protection matters, and 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.

5.4. The Data Protection Officers are 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.

5.5. Weymouth College data registration number is: Z8914348.

6. Subject Access Rights

6.1. 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 Data Protection Officer. Any member of staff receiving a SAR should forward this to the Data Protection Officer.

Consent for Processing Data

6.2. 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 Weymouth College is processing any sensitive data, as defined by the legislation.

6.3. Weymouth College 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:

- for example this statement is no longer acceptable. "*For the purposes of the General Data Protection Regulation 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."*

6.4. Weymouth College 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.

6.5. Weymouth College 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:

6.6. Weymouth College 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.

7. Fees

Normally there will be no fee charged to comply with a subject access request. However, The College reserves the right to charge a fee for data subject access requests where the request is manifestly unfounded or excessive. A "reasonable fee" for the administrative costs of complying with the request will be charged. A fee will also be payable if an individual requests further copies of their data following a request. This fee will be based on the administrative costs of providing further copies.

8. Time Limit

The College will comply without undue delay and at the latest within one calendar month of receipt of the request. The date is calculated from the day after you receive the request (whether the day after is a working day or not) until the corresponding calendar date in the next month.

9. Disclosure of Data

9.1. Only disclosures which have been notified under the College's DP notification must be made and therefore staff, students and service users should exercise caution when asked to disclose personal data held on another individual or third party.

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

9.3. Legitimate disclosures may occur in the following instances:

- the individual has given their consent to the disclosure.
- the disclosure has been notified to the OIC and is in the legitimate interests of the College.
- the disclosure is required for the performance of a contract.

9.4. 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 (CoP).

9.5. In no circumstances will Weymouth College sell any of its databases to a third party.

Publication of College Information

9.6. Weymouth College publishes various items which may include some personal data, such as:

- The internal telephone directory.
- Event information.
- 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 Weymouth College policy to offer an opportunity to opt-out of the publication of such when collecting the information.

E-mail

9.7. It is the policy of Weymouth College 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

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

10. Responsibility

- Vice Principal Funding, Systems Development, and Operations
- Clerk to the Corporation
- All College Staff

Definitions:	None.	**Who Needs to Know?**	• All College staff • Corporation Members • Parents • Students and Service users • Visitors to the College
Related Policies and Procedures:	• Acceptable Use Policy • Phone and Mobile Data Policy • Data Retention Schedule • Student References • HR Policies related to Employee Data	**Approval Date:**	March 2022
This policy was approved and adopted by: *Julia Howe* **Principal and Chief Executive Officer**			