General Data Protection Policy

TABLE OF CONTENTS

1. OVERVIEW

The College's reputation and future growth are dependent on the way it manages and protects Personal Data. As an organisation that collects, uses, and stores Personal Data about its employees, students, and suppliers etc., the College recognises its obligations under Data Protection Laws, in particular Article 5 of GDPR.

Protecting the confidentiality and integrity of Personal Data is a key responsibility of everyone within the College, and all College Personnel are required to comply with this Policy.

If you have any queries concerning this Policy, please contact our Data Protection Officer, who is responsible for ensuring the College's compliance with this Policy.

2. ABOUT THIS POLICY

This Policy (and the other policies and documents referred to in it) sets out the basis on which the College will collect and use Personal Data either where the College collects it from individuals itself, or where it is provided to the College by third parties. It also sets out rules on how the College handles, uses, transfers, and stores Personal Data.

This Policy applies to all Personal Data stored electronically, in paper form, or otherwise.

3. DEFINITIONS

3.1. **College** – Herefordshire, Ludlow and North Shropshire College, including County Training).

3.2. **College Personnel** – Any College employee, worker or contractor who accesses any of the College's Personal Data and will include employees, consultants, contractors, and temporary personnel hired to work on behalf of the College.

3.3. **Controller** – Any entity (e.g., company, organisation, public authority, or person) that makes its own decisions about how it is going to collect and use Personal Data. As an organisation, the College itself is the Controller; the role is not the legal responsibility of a particular individual.

3.4. **Data Protection Laws** – The General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA 2018)

3.5. **Data Protection Officer –** Our nominated Data Protection Officer is Clare Perez and can be contacted at dataprotection@hlcollege.ac.uk. Our Deputy Data Protection Officer is Mitchell Gardner.

3.6. **ICO** – the Information Commissioner's Office, the UK's data protection regulator.

3.7. **Registration of Data Controllers** – The college is registered with the ICO, our registration reference is Z8678471.

3.8. **EEA** – Countries in the European Economic Area**.**

3.9. **Individuals** – Living individuals who can be identified, *directly or indirectly*, from information that the College has. For example, an individual could be identified directly by name, or indirectly by gender, job role and office location (if you can use this information to work out who they are). Individuals include employees, students, parents, visitors, and potential students. Individuals also include partnerships and sole traders.

3.10. **Personal Data** – Any information about an individual which identifies them or allows them to be identified in conjunction with other information that is held. Personal data is defined very broadly and covers both ordinary personal data, e.g., personal or business contact details, through to special categories of personal

data, e.g., political opinions or religious beliefs. It also covers information that allows an individual to be identified indirectly, e.g., an ID number, location data or an online identifier.

3.11. **Processor** – Any entity (e.g., company, organisation, public authority, or person) which accesses, processes or uses Personal Data on the instruction of a Controller.

3.12. **Special Categories of Personal Data** – Personal Data that reveals a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data (i.e., information about their inherited or acquired genetic characteristics), biometric data (e.g., fingerprints, facial images), physical or mental health, sexual life or sexual orientation, and criminal record. Special Categories of Personal Data are given extra protection by Data Protection Laws.

4. COLLEGE PERSONNEL'S RESPONSIBILTIES

4.1. All College Personnel must comply with this policy.

4.2. College Personnel must ensure that they keep confidential all Personal Data that they collect, store, use and come into contact with during the performance of their duties.

4.3. College Personnel must not release or disclose any Personal Data:

- Outside the College.
- Inside the college, to College Personnel not authorised to access the Personal Data.
- Without specific authorisation from their manager or the Data Protection Officer; this includes by phone calls or in emails.

4.4. College Personnel must take all steps to ensure there is no unauthorised access to Personal Data whether by other College Personnel who are not authorised to see such Personal Data or by people outside the College.

5. DATA PROTECTION PRINCIPLES

5.1. When using Personal Data, Data Protection Laws require that the College complies with the following principles. These principles require Personal Data to be:

- Processed lawfully, fairly and in a transparent manner.

- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
- Adequate, relevant, and limited to what is necessary for the purposes for which it is being processed.
- Accurate and kept up to date, meaning that every reasonable step must be taken to ensure that Personal Data that is inaccurate is erased or rectified as soon as possible.
- Kept for no longer than is necessary for the purposes for which it is being processed.
- Processed in a manner that ensures appropriate security of the Personal Data, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organisational measures.

6. LAWFUL USE OF PERSONAL DATA

6.1. The College must have a lawful basis to collect and/or process Personal Data. The ICO has defined six lawful bases for processing, which are viewable at www.ico.org.uk.

6.2. If the College collects and/or uses Special Categories of Personal Data, it must identify both a lawful basis (Section 6.1) and a separate condition for processing under Article 9. These additional conditions for processing Special Category Personal Date are viewable at www.ico.org.uk.

6.3. The College will assess how it uses Personal Data and ensure it complies with the obligations set out in paragraphs 6.1 and 6.2. If the College changes how it uses Personal Data, the College may need to notify Individuals about the change. If, at any point, College Personnel intend to change how they use Personal Data, they must notify the Data Protection Officer so that any necessary actions can be taken.

7. PRIVACY NOTICES

7.1. Where the College collects Personal Data directly from Individuals, the College will inform them about how the College uses their Personal Data. This information is detailed in the privacy notices titled:

- *Privacy Policy - College Staff*
- *Privacy Policy - College Students*

7.2. If the College receives Personal Data about an Individual from other sources, the College will also provide the Individual with information about how the College

will use this Personal Data. This will be provided as soon as reasonably possible and in any event within one month.

8. DATA QUALITY AND ACCURACY

8.1. The College will only collect and process Personal Data to the extent that it is required for the specific purpose(s), as notified to the Individual in a privacy notice (see paragraph **Error! Reference source not found.**.1 above) or other information provided by College (e.g., the learner agreement).

8.2. All College Personnel that collect and record Personal Data shall ensure that it is recorded accurately, is kept up to date, is adequate, relevant, and limited to what is necessary in relation to the purpose for which it is collected and used.

8.3. All College Personnel that obtain Personal Data from sources outside the College should follow the guidance outlined in section 8.2, although this does not require College Personnel to independently check the Personal Data obtained.

8.4. To maintain the quality of Personal Data, all College Personnel that access Personal Data shall ensure that it is reviewed and updated to meet the criteria outlined in section 8.2. Please note that this does not apply to Personal Data which the College must keep in its original form (e.g., for legal reasons or that which is relevant to an investigation).

9. DATA RETENTION

9.1. The College will comply with Data Protection Laws and will not keep Personal Data longer than is necessary for the purpose(s) for which it was collected.

9.2. The College will document the retention rules for the Personal Data that it holds in a Data Retention Policy. This will include retention periods for the different types of Personal Data, the reasons for those retention periods, and how the College securely deletes Personal Data at the end of those periods.

9.3. If any College Personnel has a query concerning the College's retention practices or, if they feel, that a particular item of Personal Data needs to be kept for more or less time than the retention period set as out in the Data Retention Policy (e.g., because there is a requirement of law), they should contact the Data Protection Officer for guidance.

10. DATA BREACH AND SECURITY

10.1. The College's reputation and future growth are dependent on the way it manages and protects Personal Data. As an organisation that collects and uses Personal

Data, the College takes seriously its obligations to keep that Personal Data secure and to deal with security breaches relating to Personal Data when they arise.

10.2. A Personal Data breach is defined very broadly and is effectively any failure to keep Personal Data secure, which leads to the accidental or unlawful loss (including loss of access to), destruction, alteration, or unauthorised disclosure of Personal Data.

10.3. Due to implications of data breach the College has put in place a dedicated policy to address these matters. Please see the Data Breach Notification Policy for further information.

11. DATA PROCESSORS AND SHARING

11.1. There are occasions where the Personal Data that the College holds is processed by an external party. Where this happens, the external party is acting as the College's Data Processor and is bound by the College's Data Protection Policy.

11.2. Where the College shares information with others, e.g., awarding/funding bodies and local authorities, the basis of the sharing is either covered in the College's contract with that organisation or is the subject of a Sharing Agreement.

11.3. Sometimes the College will share information because it is obliged to do so by law, e.g., a request from the Police during their enquiries into a crime. In these situations, the College will not seek the permission from the individual concerned; neither will the College tell them that it has provided the information.

11.4. If a student or member of staff wants the College to share data with someone else, e.g., a solicitor, this can only be done with the student or member of staff's written consent. All such requests are dealt with under the Subject Access Request Procedure.

11.5. For learners under the age of 18 at the start of their programme of study, key data may be shared with parents or guardians.

11.6. Sometimes the College receives requests for information under the Freedom of Information Act. The College recognises the need to balance the confidentiality of personal data against a desire to be open and transparent about its activities. However, when these two factors conflict, greater weight will always be given to data confidentiality.

12. INDIVIDUALS' RIGHTS

GDPR gives individuals more control about how their data is collected and stored and what is done with it.

12.1. **Subject Access Requests**

- Individuals have the right to access and receive a copy of their Personal Data. Individuals can make a SAR verbally or in writing via the College's Data Protection Officer.
- The College will respond within one month of receipt of request, unless the request is complex, where the time limit can be extended by another two months. In most circumstances the College will not charge a fee.

12.2. **Right of Erasure (Right to be Forgotten)**

This is a limited right for individuals to request the erasure of Personal Data concerning them where:

- The use of the Personal Data is no longer necessary.
- The individual withdraws their consent or otherwise objects, and there are no other legal grounds for the processing.
- The Personal Data has been unlawfully processed.
- The Personal Data must be erased for compliance with a legal obligation.
- The Personal Data is being used for direct marketing purposes and the individual objects to that processing.

12.3. **Right of Data Portability**

An individual has the right to request that Personal Data concerning them is provided to them in a structured, commonly used, and machine-readable format where:

- The processing is based on consent or on a contract.
- The processing is carried out by automated means (i.e., excluding paper files).

12.4. **The Right of Rectification and Restriction**

Individuals are given the right to have inaccurate Personal Data rectified, and/or completed if it is incomplete. The College will respond within one month and, if refused, the Data Protection Officer will explain why.

Finally, individuals have the right to restrict the College processing their Personal Data in certain circumstances. This means that an individual can limit the way that the College uses their data. This is an alternative to requesting the erasure of their data.

13. MARKETING AND CONSENT

13.1. The College may sometimes contact Individuals to send them marketing or to promote the College. This will always be done in a legally compliant manner and Individuals can withdraw their consent for this at any time.

13.2. The College is also aware of its legal obligations regarding all electronic communications and will follow the Privacy and Electronic Communications Regulations (PECR).

14. DATA PROTECTION IMPACT ASSESSMENTS (DPIAs)

14.1. A Data Protection Impact Assessment (DPIA) is a process which helps to identify and mitigate potential risks to privacy and compliance with Data Protection Laws when processing Personal Data.

14.2. The College will perform a DPIA before processing any Personal Data that is likely to result in a high risk to the rights and freedoms of Individuals (e.g., biometric data).

14.3. The College may also perform DPIA where it is good practice to do so, e.g., before a major project which requires the processing of Personal Data.

14.4. All DPIAs must be reviewed and approved by the Data Protection Officer. The ICO's standard DPIA template is available from www.ico.org.uk.

15. TRANSFERRING DATA OUTSIDE THE EEA

15.1. Data Protection Laws impose strict controls on Personal Data being transferred outside the EEA. Transfer includes sending Personal Data outside the EEA but also includes storage of Personal Data or access to it outside the EEA. It needs to be thought about whenever the College appoints a supplier outside the EEA or the College appoints a supplier with group companies outside the EEA which may give access to the Personal Data to staff outside the EEA.

15.2. So that the College can ensure it is compliant with Data Protection Laws, College Personnel must not export Personal Data unless it has been approved by the Data Protection Officer.

15.3. College Personnel must not export any Personal Data outside the EEA without the approval of the Data Protection Officer.

16. PENALTIES AND FINES FOR NON-COMPLIANCE

16.1. The Information Commissioner has the power to impose fines for failure to comply with the UK GDPR. The standard maximum fine is up to £8.7M or 2% of annual turnover, with a higher maximum of up to £17.5M or 4% of annual turnover.

17. RELATED POLICIES

17.1. Please refer to the following policies for further information on how Herefordshire, Ludlow and North Shropshire College manage personal data:

- *Personal Data Breach Notification Policy*
- *Privacy Policy - College Staff*
- *Privacy Policy - College Students*