DATA PROTECTION POLICY (UK GDPR)

Purpose of Policy/Document	To ensure that HoW College satisfies the requirements of the General Data Protection Regulations (UK GDPR). To safeguard the personal information of students, staff and any other people for whom the College collects or processes personal data, and to make them aware of their rights under UK GDPR. To make staff and students aware of the importance of protecting personal data, and informing them of the actions they need to take to make sure the College complies with UK GDPR.
Target Audience (staff/students/ visitors/contractors)	The policy applies to all staff and any others who act on behalf of the College, and to anyone whose personal data is processed by the College. The policy also applies to partners who process personal data held on behalf of the College.
Particular Legal Requirements/Issues outside of EDD	Requirement to satisfy the Data Protection Act 2018
Links with Other Policies/Documents	Document Retention Policy; Subject Request Procedures; Privacy Impact Assessment; Safeguarding Policy; Information Security Procedures; Staff Reference Procedure; Staff Code of Conduct.
For completion by The Executive	
Policy/Document Reference No.	MIS01
Category	MIS
Owner (job title)	Data Protection Officer
Issue Date	April 2025
Review Date	April 2027
Postholder Responsible for Review (job title)	VP – Finance and Corporate Operations
Authorised By: (SLT/Corporation)	Corporation – April 2025
Communicated via/Location: (Policy Acceptance software/website/ portal etc)	Portal; Website; Cascade.
Equality Impact Assessment Statement	The Equality Act 2010 does not require public authorities to carry out EIAs by law. The College does however, carefully consider the impact, when creating or amending its policies, on all concerned parties regarding Equality, Diversity and Inclusion and records this at SLT meetings in order to demonstrate compliance with Public Sector Equality Duty (PSED).

Heart of Worcestershire College – Data Protection Policy (UK GDPR)

1 Introduction

The College recognises the importance of personal data to individuals and treats their data with care and respect. It also seeks to comply with all aspects of data protection legislation including the Data Protection Act 2018 and the General Data Protection Regulation (UK GDPR), both of which came into force in May 2018.

2 Who we are and how to contact us

Heart of Worcestershire College (HoW College) provides Further and Higher Education. It is based in Worcestershire, with campuses in Bromsgrove, Redditch, Malvern and Worcester.

Contact details will be provided on each privacy notice and on the website www.howcollege.ac.uk.

3 UK GDPR Principles

Article 5 of the UK GDPR requires that personal data shall be:

a) processed lawfully, fairly and in a transparent manner in relation to individuals;
b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which they are processed, is erased or rectified without delay;
e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the UK GDPR in order to safeguard the rights and freedoms of individuals; *and*
f) 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.

In addition, Article 5(2) of the UK GDPR states that the controller (i.e. the College) will be responsible for, and able to demonstrate compliance with these principles.

4 Responsibilities

The College takes responsibility for protecting personal data, and for complying with the law, extremely seriously. In order to achieve this, compliance is monitored by the College corporation.

In addition, the Senior Leadership Team will set targets and monitor the achievement of those targets on various aspects of compliance including, training, privacy notices, compliance checks, subject access requests, breach reports and partner compliance.

The College employs a Data Protection Officer (DPO), as required by the UK GDPR, to monitor compliance, policies, training and audits, to provide advice, to act as a contact with ICO and to monitor risk associated with College processes.

All staff receive UK GDPR training appropriate to their role, and are required to take responsibility for personal data that they collect or process.

5 The Legal Basis for Collecting and Processing Data

The lawful bases for processing are set out in Article 6 of the UK GDPR. At least one of these must apply whenever the College processes personal data:

(a) Consent: the individual has given clear consent for you to process their personal data for a specific purpose. This must be freely given, fully understood, and the subject must "opt in" to consent. Consent will only be used as a lawful reason for processing if none of the other reasons applies.

(b) Contract: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.

(c) Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations). For HoW College, these legal obligations would include safeguarding, meeting the requirements of the equality act, or meeting employees' rights. In particularly, the majority of the student personal data we collect is legally required by our funding or regulatory bodies, i.e. ESFA, DfE or the OfS.

(d) Vital interests: the processing is necessary to protect someone's life.

(e) Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law. As a College, our public task is to provide education and training, and any personal data necessary to achieve those ends will be lawful for this reason.

(f) Legitimate interests: the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. Since HoW College is a Public Authority, the College cannot use this as a lawful reason to process data for its core purpose of education and Training.

6 Processing Personal and Special Category Data

Special Categories of data include, but are not limited to:

- race;
- ethnic origin;
- politics;
- religion;
- trade union membership;
- genetics;

- biometrics (where used for ID purposes);
- health;
- sex life;
- sexual orientation.

Special category data requires further conditions to lawfully process under Article 9 of the UK GDPR. The lawful reasons that the College are most likely to use are:

a) The data subject has given explicit consent to the processing of those personal data for one or more specified purposes.
b) Processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law. The College has a lot of such obligations, including the equality act and employment law.
c) Processing is necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving consent. However, this would only be used in very serious situations.
d) Processing is necessary for reasons of substantial public interest,

7 Criminal Convictions

We will collect details of criminal convictions and carry out DBS checks for all staff and certain visitors, e.g. regular contractors, volunteers, governors, as required by law.

We will collect details of criminal convictions and carry out DBS checks for learners on courses such as Early Years, where required for safeguarding reasons in order for the learners to gain the necessary experience of working with young or vulnerable people. For other learners, we will require them to discuss convictions or offences which might be of relevance to the safeguarding and protection of others in the College, particularly young people. Where the College deems it necessary for the reasons mentioned, we will record and process that information as necessary.

8 Privacy by Design

Under the UK GDPR, the College has a general obligation to implement technical and organisational measures to show that it has considered and integrated data protection into its processing activities.

The College has many IT systems and processes which have been adapted as appropriate to meet UK GDPR requirements. Where we build new IT systems for storing or accessing personal data, develop policies or strategies that have privacy implications, embark on a new data sharing initiative, or use data for new purposes, we will carry out a Privacy Impact Assessment (PIA) to identify and minimise the privacy risks. The College has published a PIA procedure.

9 Records of Processing Activities

The College has compiled an Information Asset Register (IAR) in order to identify and track all personal data collected and processed by the College.

To ensure the accuracy and completeness of our data records, the IAR shall be reviewed and updated on an annual basis. This review will be conducted by the Data Protection Officer (DPO). The review process will include:

- Verifying the current status of all information assets.

- Ensuring that all new information assets are documented.
- Updating any changes to existing information assets.
- Confirming that all information assets comply with current data protection regulations.

The annual review aims to maintain the integrity and security of our data management practices, ensuring ongoing compliance with the UK GDPR and other relevant data protection laws.

In addition, the College has created a register of all forms, both manual and electronic, used to collect personal data. These registers will be maintained and reviewed in order to enable the College to audit the personal data held and its security, minimise data collected, monitor deletion dates ensure that privacy notices (PN's) are provided whenever personal data is collected, enable subject access requests to be carried, to monitor the impact of any breach, and to monitor all our partners and their role in sharing and processing personal data.

10 Data Protection Officer

The College employs a Data Protection Officer (DPO), as detailed in the UK GDPR to monitor compliance, policies, training and audits, to provide advice, to act as a contact with ICO and to monitor risk associated with processing operations. The Data Protection Officer can be contacted by emailing dataprotection@howcollege.ac.uk or by writing to the College at the address given under College contacts.

11 Subject Rights

Under UK GDPR, data subjects have the right to:

- Access and obtain a copy of their data on request;
- Require the College to change incorrect or incomplete data;
- Require the College to delete or stop processing their data, for example where the data is no longer necessary for the stated purposes of processing;
- Object to the processing of their data where the College is relying on its legitimate interests as the legal ground for processing. The College will only use "legitimate interests" as grounds for processing in a very few situations;
- Prevent processing for the process of direct marketing, although we will continue to contact where necessary in order to provide learning – for example to notify them about a change of class. Also, the College will need to contact them to obtain destination information as required by ESFA or HEFCE.

The College provides detailed information and a subject request form on its website. The College will make as much personal data as possible available for students or staff to check whenever they choose via the College portal.

The College has a form outlining the rights of data subjects and which explains how they can exercise their rights. This can be obtained on the College website, by contacting dataprotection@howcollege.ac.uk or by contacting the College reception for anyone who does not have access to the website or email.

12 Privacy Notices

At each point at which the College collects personal data, it will provide a privacy notice which will:

- Provide details of the College and provide contact details;

- Explain what personal data is being collected and processed, and why;
- Explain the lawful basis for collecting data, which may include consent;
- Explain where we obtain data from;
- Provide details of how we store the data and who has access to it;
- List organisations who may need to share the data, and provide appropriate sharing agreements, for example with the Department for Education or the Office for Students;
- Detail any data stored outside of the EU;
- Provide details of who long the data is retained;
- Provide details of the rights of the subject, how to exercise their rights, and details of who to complain to;
- Consequences of not providing personal data (other than data requiring consent);
- Details of any automated decision making.

There will privacy notices for each group of people who provide the College with personal data. This includes students who apply to courses, students who enrol, staff who apply, staff who are employed, visitors and people who make enquiries by post, phone or email.

13 International Transfers

The College does not store any data outside the EU. It will monitor partners and will require assurances that either they do not store College personal data abroad outside of areas covered by UK GDPR, or, if they do, the standards of data protection are at least as good as those required by UK GDPR.

14 Data Retention & Schedule

Full details are provided in the Document Retention Policy. Privacy notices will indicate retention periods. Data provided by consent will be deleted on request, however, requests to delete personal data cannot be enacted where the data has been retained for other lawful reasons, for example, where the College is required to retain data to meet DfE or ESFA requirements or to enable it to carry out its duties.

15 Data Breaches

The College has an Information Security Procedure designed to quickly identify if personal data has been compromised, its significance, who is affected, what actions are required, and whether the ICO needs to be informed. The process will immediately escalate to Vice Principal level if appropriate. The process includes a log of any data breaches, actions required and action taken. All breaches will be logged and reviewed.

ICO must be informed of details within 72 hours of the College becoming aware of any non-minor breach of personal data. ICO require information about the date and time or the breach, when it was detected, information about the type of breach and about the information concerned, the number of individuals affected, and the possible effect on them, measure taken to mitigate effects, and information about the notice to customers.

The Information Commissioner's Office (ICO) has the authority to impose fines for data breaches. These fines can amount to up to £17.5 million or 4% of the annual turnover of the organisation, whichever is higher. The ICO's fining guidance outlines how penalties are calculated and emphasises the importance of having robust breach detection, investigation, and internal reporting procedures in place. This ensures that breaches are detected and reported in a timely manner, and that all

necessary details are provided to the ICO

Failure to report a data breach when required to do so could result in a fine. This is in addition to any fines that may be imposed for the breach itself. If the breach is likely to result in a high risk to the rights and freedoms of individuals, those affected must also be informed without undue delay

16 Marketing

Marketing by electronic means is covered by the Privacy and Electronic Communications Regulations (PECR) which sit alongside the Data Protection Act. They give people specific privacy rights in relation to electronic communications. In particular, subjects must provide opt-in to consent to receiving emails or texts for general marketing or surveys and can request opt-out at any subsequent time.

This does not apply to communications such as emails or texts which are required to carry out our lawful tasks, e.g. an email to notify a student of the date and time of their lesson, or to gather information required by law, such as destinations. "Soft" opt-in may apply when providing information deemed directly relevant to an application or enquiry, providing the College makes it simple to opt-out at any stage.

The College will ensure that it has consent to send electronic marketing information. All marketing information sent will provide simple instructions about how to opt-out from future communications.

17 Students under 18 on 1st September

The College recognises the importance of involving parents and carers in the support of students who are aged under 18 on 1st September in the relevant academic year. However, it is also mindful of the privacy rights of such students under UK GDPR.

When prospective students in this age group apply to courses at the College, or when such students enrol to courses, we will encourage them to consent to us sharing details of progress with their parents, and to let us notify parents/carers about parents' evenings, interviews, open days and so on. We will also encourage them to give consent to sharing special details with parents and carers.

We will collect emergency contact details for all young students in this age group. This information would only be used to protect the vital interests of these young students. Emergency details for adult students will be provided by consent.

UK GDPR requires that privacy notices are fully understood. Where we feel that a young or vulnerable student might not fully understand the implications of the privacy notices, we will provide assistance to explain it.

18 Partnerships and Data Sharing Agreements

Whenever the College, in the position of data controller, uses a partner to process data, it will have a written contract in place that complies with the requirements listed by ICO. This is to ensure both parties understand their responsibilities and liabilities. As a College, we are liable for their compliance with the UK GDPR and we will only appoint processors who can provide sufficient guarantees that the requirements of the UK GDPR will be met and the rights of data subjects protected. All processors will be required to act only on the documented instructions of the College.

If the College processes data for another controller, it will comply with the ICO checklist of UK GDPR requirements.

Where the College is joint controller of data, for example, with agencies such as ESFA, OfS, LRS, WCC, and Awarding Organisations, the College will provide access to the privacy notices published by these organisations. These can be found on the College website, by emailing dataprotection@howcollege.ac.uk, or by enquiring at reception.

Appendix A - Definition of terms in this policy

Below are explanations of some of the terms in this policy.

- **Data Protection Act 1998 (DPA)** – legislation that governed the use of personal information between 1998 and May 25th 2018.
- **General Data Protection Regulations (UK GDPR)** – legislation introduced on 25th May 2018 which replaces the DPA.
- **Personal information** - information, alone or combined with other information, which may identify living people. This could include, for example, IP addresses, or student identification number. We do not consider personal information to include information that has been anonymised, providing it does not allow them to be identified.
- **Data Owner** - individual or department within an organisation who holds authoritative rights over specific datasets. They are accountable for the data within their area of expertise and understand how it is generated, used, and managed
- **Special category personal information -** personal information considered especially sensitive as defined by the UK GDPR. This includes racial or ethnic origin, religious beliefs or beliefs of a similar nature, trade union membership, physical or mental health condition, sexual life. We will also treat criminal proceedings or convictions within this category.
- **Data Protection Officer (DPO) –** a College employee identified within UK GDPR who has an independent oversight of the implementation of UK GDPR within the College.
- **Subject Access Request (SAR) –** a request by an individual to access details of their personal data held and processed, for changes to correct data or for deletion of data.
- **Article 6 –** refers to the lawful reasons for collecting and processing data in the UK GDPR.
- **Article 9 –** refers to the lawful reasons for collecting and processing special category data in UK GDPR (a lawful reason in article 6 is also needed).
- **Article 10 –** refers to the lawful reasons for collecting and processing criminal conviction data in UK GDPR (a lawful reason in article 6 is also needed).
- **ICO –** Information Commissioner's Office – the government office which advises on, and enforces UK GDPR.
- **Privacy Impact Assessment (PIA) –** an assessment of the risks to personal data.
- **Privacy Notice –** details the lawful reasons for collecting and processing personal data in a form or on a web page, in addition to giving information about data subjects rights.
- **Privacy and Electronic Communications Regulations (PECR) -** these sit alongside the Data Protection Act. They give people specific privacy rights in relation to electronic communications.
- **Data Subject –** a data subject is anyone whose personal data is processed by the College.
- **Data Controller –** the Data Controller is the organisation which decides the purpose for which any personal data is to be processed and the way in which it is to be processed.
- When we refer to **the website**, this can be found at www.howcollege.ac.uk which has a section dedicated to personal data privacy and UK GDPR.
- **DBS Checks -** employers can only check the criminal record of someone applying for certain roles, for example in healthcare or childcare. The Disclosure and Barring Service (DBS) helps employers make safer recruitment decisions and prevent unsuitable people from working with vulnerable groups, including children.
- **WCC – Worcestershire County Council –** the Council has a statutory role with regard to the education and training of 16-18 year olds, and with regard to Child Protection and Safeguarding.