

GDPR Policy

General Data Protection Policy

<i>Reference and Version number</i>	<i>General Data Protection Policy V1.2025</i>
<i>Author</i>	<i>Data Protection Officer</i>
<i>Designated Owner</i>	<i>Data Protection Officer</i>
<i>Approving body</i>	<ul style="list-style-type: none"> • <i>Policy and Procedure Panel</i> • <i>SLT</i> • <i>Board of Governors</i>
<i>Date Approved including Impact Assessment</i>	<i>December 2025</i>
<i>Linked policies and procedures</i>	<ul style="list-style-type: none"> • <i>Rights of Individuals Policy</i> • <i>Personal Data Breach Notification Policy</i> • <i>Retention and Disposal of Information Policy</i> • <i>IT Acceptable Use Policy</i>
<i>Date of next review</i>	<i>December 2026</i>

1. Introduction

- 1.1 The College's reputation and future growth are dependent on the way the College manages and protects Personal Data. Protecting the confidentiality and integrity of Personal Data is a key responsibility of everyone within the College.
- 1.2 As an organisation that collects, uses and stores Personal Data about its employees, suppliers (sole traders, partnerships or individuals within companies), students, governors, parents and visitors, the College recognises that having controls around the collection, use, retention and destruction of Personal Data is important in order to comply with the College's obligations under Data Protection Laws and in particular its obligations under Article 5 of GDPR.
- 1.3 The College has implemented this Data Protection Policy to ensure all staff are aware of what they must do to ensure the correct and lawful treatment of Personal Data. This will maintain confidence in the College and will provide for a successful working and learning environment for all.
- 1.4 Staff will receive a copy of this Policy when they start and may receive periodic revisions of this Policy. This Policy does not form part of any member of the Staff's contract of

employment and the College reserves the right to change this Policy at any time. All members of Staff are obliged to comply with this Policy at all times.

- 1.5 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

- 2.1 This policy sets out the accountability and responsibilities of the College, employees, contractors, agency staff, volunteers, students and other relevant parties, in ensuring compliance with data protection and the security of personal data as required under any and all applicable legislation. This includes, but is not limited to;

- UK GDPR (United Kingdom General Data Protection Regulation)
- Data Protection Act 2018 o Freedom of Information Act 2000
- Equality Act 2010 o Computer Misuse Act 1990
- Fraud Act 2006 (with regards to phishing and identity theft and fraud)
- Theft Act (with regards to electronic theft)
- Network and Information Systems and Regulations 2018
- Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR)
- Investigatory Powers Act 2016 (which replaces the Regulation of Investigatory Powers Act 2000)

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

3. Definitions

- 1.1 **College** – Hertford Regional College, Ware Campus, Scotts Rd, Ware, Herts, SG12 9JF

- 1.2 **Staff** – 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.

- 1.3 **Controller** – Any entity (e.g. company, organisation or person) that makes its own decisions about how it is going to collect and use Personal Data.

A Controller is responsible for compliance with Data Protection Laws. Examples of Personal Data the College is the Controller of include employee details or information the College collects relating to students. The College will be viewed as a Controller of Personal Data if it decides what Personal Data the College is going to collect and how it will use it.

A common misconception is that individuals within organisations are the Controllers. This is not the case it is the organisation itself which is the Controller.

- 1.4 **Data Protection Laws** – All applicable laws relating to the collection and use of Personal Data and privacy and any applicable codes of practice issued by a regulator including in the UK, the Data Protection Act 2018 and UK GDPR.

- 1.5 **Data Protection Officer** – Our Data Protection Officer is Olive Oliver, and can be contacted at: 01992 411999, ooliver@hrc.ac.uk.

- 1.6 **EEA** – Austria, Belgium, Bulgaria, Croatia, Republic of Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden and the UK.
- 1.7 **ICO** – the Information Commissioner’s Office, the UK’s data protection regulator.
- 1.8 **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.
- 1.9 **Personal Data** – Any information about an Individual (see definition above) which identifies them or allows them to be identified in conjunction with other information that is held. It includes information of this type, even if used in a business context.

Personal data is defined broadly and covers things such as name, address, email address (including in a business context, email addresses of Individuals in companies such as `firstname.surname@organisation.com`), IP address and also more sensitive types of data such as trade union membership, genetic data and religious beliefs. These more sensitive types of data are called “Special Categories of Personal Data” and are defined below. Special Categories of Personal Data are given extra protection by Data Protection Laws.

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

A Processor is a third party that processes Personal Data on behalf of a Controller. This is usually as a result of the outsourcing of a service by the Controller or the provision of services by the Processor which involve access to or use of Personal Data. Examples include: where software support for a system, which contains Personal Data, is provided by someone outside the business; cloud arrangements; and mail fulfilment services.

- 3.11. **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 (i.e. information about their physical, physiological or behavioural characteristics such as facial images and fingerprints), physical or mental health, sexual life or sexual orientation and criminal record. Special Categories of Personal Data are subject to additional controls in comparison to ordinary Personal Data.

4. Staff’s General Obligations

- 4.1 All Staff must comply with this policy.
- 4.2 Staff 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 Staff must not release or disclose any Personal Data:
- outside the College; or
 - inside the college to Staff 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. Staff must take all steps to ensure there is no unauthorised access to Personal Data whether by other Staff who are not authorised to see such Personal Data or by people outside the College.

5. Data Protection Principles

- The College's processing of personal data must be conducted in accordance with the data protection principles as set out in Article 5 of the UK GDPR.
 - The College is committed to upholding the data protection principles. All personal data under the College's control will be processed in accordance with the principles.
- 5.1 When using Personal Data, Data Protection Laws require that the College complies with the following principles (A – D). 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; and
 - 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.
- 5.2 The College will implement all reasonable measures to maintain compliance with the above principles.
- All data must be collected and processed lawfully, fairly, and transparently.
 - May only collect data for specified explicit, and legitimate purposes that have been made clear to data subjects at the start of the processing.
 - The college and the subsidiary company are required to ensure that adequate, relevant, and limited data is used where necessary in relation to the purposes for which they are processed. All data collection should be minimised.
 - Personal data should be processed only if the purpose of the processing could not reasonably be fulfilled by other means.

5.3 Principle (E) – Retention and Destruction of Records

- The College will not keep personal data in a form that permits identification of data subjects for a longer period than is necessary, in relation to the purpose(s) for which the data was originally collected.
- The College reserve the right to store data for longer periods if the personal data is processed solely for archiving purposes in the public interest, statistical purposes, scientific or historical research purposes, or if necessary to fulfil contractual obligations. This is subject to the implementation of appropriate technical and organisational measures to safeguard the rights and freedoms of the data subject.
- The retention period for each category of personal data will be set out in the Retention Policy along with the criteria used to determine this period including reference to any statutory obligations.
- When disposing of personal data, the College will:
 - o only delete or dispose of data in line with the Retention Policy, or in response to a right of erasure request where the conditions set out in Articles 17 and 19 of the UK GDPR are met.
 - o ensure that paper-based records are shredded or disposed of by the approved contractors.
 - o ensure that hard drives are destroyed by approved contractors as the College do not have the facilities to do so to the required standard in house. The disposal of hard drives should also comply with the Waste Electrical and Electronic Equipment Regulations 2013.
 - o appoint contractors responsible for data destruction that, at a minimum, meet the criteria identified as being necessary to meet the legal requirements, in addition to data protection legislation, and all other applicable legalisation.
 - o review the criteria for the disposal of personal data prior to the commencement of any applicable contracts.

5.4 Principle (F) – Information Security

- The College continuously seek to develop and implement measures that ensure a high level of security for personal and confidential data and to maintain a secure environment for information held both manually and electronically.
- All personal data should be accessible only to those who need to use it, with access granted in line with the remits of an individual's job role or in accordance with data subject rights.
- All paper-based personal data is to be kept in rooms with key locks or centralised access control, and stored in locked units including, but not limited to, lockable drawers, filing cabinets and cabinets.
- All electronically held data is processed as per the details contained within the College's ICT Policies.

6. Lawful use of Personal Data

6.1 Any personal data processed by the College must be done so in accordance with one of the six lawful bases defined in Article 6 of the UK GDPR.

6.2 In order for the College to fulfil its obligations and business requirements, the most appropriate lawful basis must be identified for each task. The lawful basis must be documented in the Records of Processing Activities as per Article 30 of the UK GDPR.

- 6.3 The processing of special category data is covered under section 6 Special Categories of Data.
- 6.4 The College accepts that no matter how urgent the data collection, processing or sharing is, the Article 6 of the UK GDPR lawful basis, and any associated conditions, must be identified, met and documented beforehand. Failure to do so is a breach of the data protection legislation, and significantly increases the risks to data subject's rights and freedoms.
- 6.5 In accordance with the Equality Act 2010, the College and the subsidiary company acknowledges that data subjects can reserve the right to not disclose personal data relating to protected characteristics.
- 6.6 Consent - the College recognises that for consent to be valid as lawful basis, the requirements of Articles 6-8 of the UK GDPR must be met. The College acknowledge that when using consent as a lawful basis, the data subject must have the option to easily withdraw their consent.

7. SPECIAL CATEGORIES OF DATA

- 7.1 The College understands that special category data is personal data which requires additional protection because it is sensitive and poses the greatest risk to individuals' risk and freedoms if compromised.
- 7.2 Article 9 of the UK GDPR defines the ten special categories of data as personal data pertaining to an individual's:
- racial or ethnic origin;
 - political opinions;
 - religious or philosophical beliefs;
 - trade union membership;
 - genetic data;
 - biometric data (where used for identification purposes);
 - health;
 - sex life;
 - sexual orientation.
- 7.3 Any special category data processed by the College must be done so in accordance with an identified lawful basis under Article 6 of the UK GDPR and a separate condition for processing identified under Article 9 UK GDPR.
- 7.4 In addition to the requirements listed in Article 9 of the UK GDPR, under Part 1 and 2 of Schedule 1 of the Data Protection Act, if the College relies on condition:
- (b), (h), (i) or (j) the College acknowledge that the associated conditions and safeguards need to be met before processing the data.
 - (g) the College acknowledge that one of 23 specific substantial public interest conditions set out need to be met before processing the data.
 - (b) or (g) the College are required to complete an 'appropriate policy document' before processing the data.
- 7.5 The College accept that no matter how urgent the requirement is to collect, process or

share special category data, the Article 6 and 9 of the UK GDPR lawful bases, and any associated conditions, must be identified, met and documented beforehand. Failure to do so is a breach of the data protection legislation, and significantly increases the risks to data subject's rights and freedoms.

- 7.6 The College will take measures to ensure that special category data is necessary for the purposes identified and that there is no other reasonable and less intrusive way to achieve that purpose.
- 7.7 If the College cannot suitably identify, and justify, why special category data is required, the College will not proceed with the processing.

8. Criminal Convictions Personal Data

- 8.1 The College understand that information pertaining to criminal convictions is personal data; and no matter how urgent the need is for criminal convictions data to be collected, processed or shared, additional protections are required because of the sensitivity and increased risk to individuals' rights and freedoms if compromised.
- 8.2 Prior to processing criminal convictions data, the College will identify and document accordingly:
- the applicable condition from Article 10 of the UK GDPR and identify if it is processing the data in an official capacity or under a condition in
 - Schedule 1 of the Data Protection Act 2018;
 - the lawful basis from Article 6 and 9 of the UK GDPR;
 - how it is complying with the Rehabilitation of Offenders Act 1974 (ROA) and Disclosure and Barring Service (DBS).
- 8.3 If the College cannot suitably identify, and justify, why criminal convictions data is required, the College will not proceed with the processing.

9. Transparent Processing – Privacy Notices

- 9.1 Where the College collects Personal Data directly from Individuals, the College will inform them about how the College uses their Personal Data. This is in a privacy notice. The College has adopted the following privacy notices: HRC General Privacy Notice.
- 9.2 If the College receives Personal Data about an Individual from other sources, the College will provide the Individual with a privacy notice about how the College will use their Personal Data. This will be provided as soon as reasonably possible and in any event within one month.
- 9.3 If the College changes how it uses Personal Data, the College may need to notify Individuals about the change. If Staff therefore intend to change how they use Personal Data please notify the Data Protection Officer who will decide whether the Staff's intended use requires amendments to be made to the privacy notices and any other controls which need to apply.

10. Data Quality

- 10.1 Data Protection Laws require that the College only collects and processes Personal Data to the extent that it is required for the specific purpose(s) notified to the Individual in a privacy notice (see paragraph 9 above) and as set out in the College's record of how it uses Personal Data. The College is also required to ensure that the Personal Data the College holds is accurate and kept up to date.
- 10.2 All Staff that collect and record Personal Data shall ensure that the Personal Data is recorded accurately, is kept up to date and shall also ensure that they limit the collection and recording of Personal Data to that which is adequate, relevant and limited to what is necessary in relation to the purpose for which it is collected and used.
- 10.3 All Staff that obtain Personal Data from sources outside the College shall take reasonable steps to ensure that the Personal Data is recorded accurately, is up to date and limited to that which is adequate, relevant and limited to what is necessary in relation to the purpose for which it is collected and used. This does not require Staff to independently check the Personal Data obtained.
- 10.4 In order to maintain the quality of Personal Data, all Staff that access Personal Data shall ensure that they review, maintain and update it to ensure that it remains accurate, up to date, adequate, relevant and limited to what is necessary in relation to the purpose for which it is collected and used. 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).
- 10.5 The College recognises the importance of ensuring that Personal Data is amended, rectified, erased or its use restricted where this is appropriate under Data Protection Laws. The College has a Rights of Individuals Policy and a Rights of Individuals Procedure which set out how the College responds to requests relating to these issues. Any request from an individual for the amendment, rectification, erasure or restriction of the use of their Personal Data should be dealt with in accordance with those documents.

11. Personal Data Retention

- 11.1 Data Protection Laws require that the College does not keep Personal Data longer than is necessary for the purpose or purposes for which the College collected it.
- 11.2 The College has assessed the types of Personal Data that it holds and the purposes it uses it for and has set retention periods for the different types of Personal Data processed by the College, the reasons for those retention periods and how the College securely deletes Personal Data at the end of those periods. These are set out in the Data Retention Policy.
- 11.3 If Staff feel that a particular item of Personal Data needs to be kept for more or less time than the retention period set out in the Data Retention Policy, for example because there is a requirement of law, or if Staff have any questions about this Policy or the College's Personal Data retention practices, they should contact the Data Protection Officer for guidance.

12. Data Security

12.1 The College takes information security very seriously and the College has security measures against unlawful or unauthorised processing of Personal Data and against the accidental loss of, or damage to, Personal Data. The College has in place procedures and technologies to maintain the security of all Personal Data from the point of collection to the point of destruction.

13. Data Breach

13.1 Whilst the College takes information security very seriously, unfortunately, in today's environment, it is possible that a security breach could happen which may result in the unauthorised loss of, access to, deletion of or alteration of Personal Data. If this happens there will be a Personal Data breach and Staff must comply with the College's Data Breach Notification Policy.

13.2 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. Whilst most Personal Data breaches happen as a result of action taken by a third party, they can also occur as a result of something someone internal does.

13.3 The **UK GDPR** and DPA 2018 set a maximum **fine** of £17.5 million or 4% of annual global turnover – whichever is greater – for infringements.

13.4 There are three main types of Personal Data breach which are as follows:

- **Confidentiality breach** - where there is an unauthorised or accidental disclosure of, or access to, Personal Data e.g. hacking, accessing internal systems that a Staff is not authorised to access, accessing Personal Data stored on a lost laptop, phone or other device, people "blagging" access to Personal Data they have no right to access, putting the wrong letter in the wrong envelope, sending an email to the wrong student, or disclosing information over the phone to the wrong person;
- **Availability breach** - where there is an accidental or unauthorised loss of access to, or destruction of, Personal Data e.g. loss of a memory stick, laptop or device, denial of service attack, infection of systems by ransom ware, deleting Personal Data in error, loss of access to Personal Data stored on systems, inability to restore access to Personal Data from back up, or loss of an encryption key; and
- **Integrity breach** - where there is an unauthorised or accidental alteration of Personal Data.

14. Appointing Contractors Who Access the College's Personal Data

14.1 If the College appoints a contractor who is a Processor of the College's Personal Data, Data Protection Laws require that the College only appoints them where the College has carried out sufficient due diligence and only where the College has appropriate contracts in place.

14.2 One requirement of GDPR is that a Controller must only use Processors who meet the requirements of the GDPR and protect the rights of individuals. This means that data protection due diligence should be undertaken on both new and existing suppliers. Once a Processor is appointed they should be audited periodically to ensure that they are meeting the requirements of their contract in relation to Data Protection.

14.3 Any contract where an organisation appoints a Processor must be in writing.

14.4 You are considered as having appointed a Processor where you engage someone to perform a service for you and as part of it they may get access to your Personal Data. Where you appoint a Processor you, as Controller remain responsible for what happens to the Personal Data.

14.5 GDPR requires the contract with a Processor to contain the following obligations as a minimum:

- to only act on the written instructions of the Controller;
- to not export Personal Data without the Controller's instruction;
- to ensure staff are subject to confidentiality obligations;
- to take appropriate security measures;
- to only engage sub-processors with the prior consent (specific or general) of the Controller and under a written contract;
- to keep the Personal Data secure and assist the Controller to do so;
- to assist with the notification of Data Breaches and Data Protection Impact Assessments;
- to assist with subject access/individuals rights;
- to delete/return all Personal Data as requested at the end of the contract;
- to submit to audits and provide information about the processing; and
- to tell the Controller if any instruction is in breach of the GDPR or other EU or member state data protection law.

14.6 In addition the contract should set out:

- the subject-matter and duration of the processing;
- the nature and purpose of the processing;
- the type of Personal Data and categories of individuals; and
- the obligations and rights of the Controller.

15. Individuals' Rights Data Subject)

- The College acknowledges that it must comply with the eight rights set out in Articles 12-23 of the UK GDPR to data subjects, known as "Data Subjects Rights":
 - The right to be informed - The right to be told how personal data is used in clear and transparent language.
 - The right of access, also known as a data subject access request (DSAR) - The right to know and have access to the personal data held about the individual.
 - The right to rectification - The right to have personal data corrected where it is inaccurate or incomplete.
 - The right to erasure, also known as the right to be forgotten - The right to have personal data deleted.
 - The right to restrict processing - The right to limit the extent of the processing of the individual's personal data.
 - The right to data portability - The right to receive personal data in a common and machine-readable electronic format.
 - The right to object - The right to complain and to seek to prevent the processing of an individual's data.
 - Rights in relation to automated decision making and profiling - The right not to be subject to decisions without human involvement.

- The College is committed to facilitating requests made by data subjects meeting the criteria of the above rights. As such, the College will:
 - process personal data in a transparent manner.
 - uphold individuals' rights under data protection legislation and allow data subjects to exercise their rights over the personal data held about them.
 - keep records of all requests and their outcome.
 - respond to requests made under these rights based on the conditions set out in law. Not all the data subjects' rights are absolute, and depending on the circumstances, exemptions may apply.
 - instruct employees receiving any requests made in relation to data subjects' rights, to not directly respond, and refer the request to the Data Protection Officer. This is supplemented by additional reminders about this requirement during employee induction and data protection training.
 - maintain internal procedures that detail how to process each of the data subject rights.
 - take reasonable measures to require individuals to confirm their identity where it is not obvious that they are the data subject.
 - not charge a fee to data subjects for enacting these rights, unless a request is found to be "manifestly unfounded or excessive" and/or reserves the right to refuse requests that are "manifestly unfounded or excessive".
 - strive to respond to all requests made by data subjects under Articles 15-22 of the UK GDPR (rights 2-8) as per Article 12 (3) which specifies the legal timeframe as "...without undue delay and in any event within one month of receipt of the request". If a request is complex then the College will invoke its ability to extend the deadline, pursuant to the legislative requirements being met. However, in addition to the above, as per Article 12 (4) of the UK GDPR, when extreme mitigating circumstances arise that hinder the College from meeting these obligations, the College will consult with data subjects and seek advice from the ICO about how to proceed. This includes but is not limited to; unforeseen/major disasters that affect operations in line with business continuity and disaster recovery operations.
 - review all requests made under data subjects rights on a case by case basis but will apply a consistent approach.

The different types of rights of individuals are:

15.1 The Right to be Informed

The College is committed to processing personal data in a transparent manner as per Articles 12-14 of the UK GDPR. To this end, the College will produce privacy notices that:

- acknowledges the data subjects' rights;
- explains how individuals can exercise their rights;
- are available in a variety of accessible forms,
- use clear, plain, meaningful language; and
- provide all relevant information required under Article 12 of the UK GDPR and the ICO guidelines.

15.2 The Right of Access

The College is committed to providing data subjects access to data held about them as per Articles 12 and 15 of the UK GDPR. To this end, the College:

- recognises that it is a criminal offence to delete personal data relevant to a right to access request after it has been received. The College is committed to only securely disposing of personal data in line with the Retention Policy or in response to a right to erasure request where the qualifying circumstances apply.

- take all reasonable measures to not adversely affect the rights and freedoms of others when responding to SARs.
- accept a subject access request verbally or in writing. When a request is made verbally the College may ask the data subject to follow this up in writing when a request is unclear.
- The college will request confirmation of the data subjects ID and required diligence before undertaking any requests and releasing data.
- will provide all relevant information required under Article 12 and 15 of the UK GDPR and the ICO guidelines.

15.3 **The Right to Rectification**

The College is committed to ensuring that the personal data held about data subjects is accurate, in accordance with the lawful bases upon which it is collected, and where applicable, the corresponding retention period defined in law. This is done so in accordance with Articles 12 and 16 of the UK GDPR. To this end, the College:

- will take reasonable measures to ensure that personal data remain accurate, but this is dependent on the data subject providing current and correct information.
- will work with data subjects to rectify inaccuracies swiftly when errors are identified.

15.4 **The Right to Erasure**

Pursuant to Articles 17 and 19 of the UK GDPR the College will delete personal data when one or more of the conditions within Article 17 of the UK GDPR are met.

15.5 **The Right to Restrict Processing**

Pursuant to Articles 18 and 19 of the UK GDPR the College will restrict the processing of personal data when one or more of the conditions within Article 18 of the UK GDPR are met.

15.6 **The Right to Data Portability**

Pursuant to Article 20 of the UK GDPR the College will provide personal data in a secure, structured, commonly used, and machine-readable format when one or more of the conditions within Article 20 of the UK GDPR are met.

15.7 **The Right to Object**

Pursuant to Article 21 of the UK GDPR the College will stop the processing of their personal data when one or more of the conditions within Article 21 of the UK GDPR are met.

15.8 **Rights in Relation to Automated Decision Making and Profiling**

- Pursuant to Article 22 of the UK GDPR the College will ensure that it fulfils its obligations when the conditions within Article 22 of the UK GDPR are applicable.
- If the College relies upon automated decision making and profiling, the process(es) will be subject to intense scrutiny and risk assessments to ensure that there are no alternative solutions available and that data subject rights are upheld.

16. Marketing and Consent

- The College will only send electronic direct marketing communications where it is the recipient's choice to opt-in.
- The College will ensure that in all electronic direct marketing communications the recipient will have the option to opt-out. If a recipient withdraws consent, the College will action as appropriate.
- The College will only send direct marketing in accordance with data protection legislation and the Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR).

17. Automated Decision Making and Profiling

17.1 Under Data Protection Laws there are controls around profiling and automated decision making in relation to Individuals.

- **Automated Decision Making** happens where the College makes a decision about an Individual solely by automated means without any human involvement and the decision has legal or other significant effects; and
- **Profiling** happens where the College automatically uses Personal Data to evaluate certain things about an Individual.

17.2 Any Automated Decision Making or Profiling which the College carries out can only be done once the College is confident that it is complying with Data Protection Laws. If Staff therefore wish to carry out any Automated Decision Making or Profiling Staff must inform the Data Protection Officer.

17.3 Staff must not carry out Automated Decision Making or Profiling without the approval of the Data Protection Officer.

17.4 The College does not carry out Automated Decision Making or Profiling in relation to its employees.

18. Controllers and Processors

18.1 Primarily, the College is considered the data controller for personal data processed in line with operational requirements and are therefore responsible for establishing policies and procedures which ensure compliance with legislation.

18.2 For the purposes of Government funding and performance accountability, the College shares data with (and may act on behalf of) external agencies. Principally this is the Department for Education and any executive agencies it sponsors, for example the Education and Skills Funding Agency (ESFA). In these situations, the external agency acts as a data controller in their own right.

18.3 The College will only appoint processors if, and when, sufficient guarantees around compliance with the data protection legislation have been supplied.

18.4 Where a processor can demonstrate that they adhere to approved codes of conduct or certification schemes, the College will take this into consideration for choice of supplier.

18.5 Processors, working with or for the College, who have access to personal data, will be expected to comply with this policy.

18.6 When the College uses a processor, a written contract/agreement with compulsory terms as set out in Article 28 of the UK GDPR must be in place, along with any additional requirements that the College determines necessary. Any written contracts/agreements with processors will entail a clause that specifies that processors can only act on the instruction of the College also giving the College the right to audit compliance with the agreement.

19. Data Protection Impact Assessments (DPIA)

19.1 When the College considers carrying out new or amended processing activities that involve personal data, privacy issues must always be assessed and a Data Protection Impact Assessment (DPIA) must be conducted.

A DPIA is not a prohibition on using Personal Data but is an assessment of issues affecting Personal Data which need to be considered before a new product/service/process is rolled out. The process is designed to:

- describe the collection and use of Personal Data;
- assess its necessity and its proportionality in relation to the purposes;
- assess the risks to the rights and freedoms of individuals; and
- the measures to address the risks.

19.2 A DPIA must be completed where the use of Personal Data is likely to result in a high risk to the rights and freedoms of individuals.

19.3 Where the College is launching or proposing to adopt a new process, product or service which involves Personal Data, the College needs to consider whether it needs to carry out a DPIA as part of the project initiation process. The College needs to carry out a DPIA at an early stage in the process so that the College can identify and fix problems with its proposed new process, product or service at an early stage, reducing the associated costs and damage to reputation, which might otherwise occur.

19.4 Situations where the College may have to carry out a Data Protection Impact Assessment include the following (please note that this list is not exhaustive):

- large scale and systematic use of Personal Data for the purposes of Automated Decision Making or Profiling where legal or similarly significant decisions are made;
- large scale use of Special Categories of Personal Data, or Personal Data relating to criminal convictions and offences e.g. the use of high volumes of health data; or
- systematic monitoring of public areas on a large scale e.g. CCTV cameras.

19.5 All DPIAs must be reviewed and approved by the Data Protection Officer.

20. International Data Transfers

20.1 Data Protection Laws impose strict controls on Personal Data being transferred outside the UK. The College will only transfer data outside the UK in accordance with Articles 44-50 of the UK GDPR. Transfer includes sending Personal Data outside the UK but also includes storage of Personal Data or access to it outside the UK.

20.2 So that the College can ensure it is compliant with Data Protection Laws Staff must not export Personal Data outside of the UK, unless it has been approved by the Data Protection Officer.

20.3 Staff must not export any Personal Data outside the EEA without the approval of the Data Protection Officer.

21. Accountability, Roles and Responsibilities

21.1 Data Protection Officer(DPO)

- The registered Data Protection Officer (DPO) acts for the College.
- As prescribed under Article 39 of the UK GDPR, the following duties are within the responsibility and remit of the DPO:
 - Champion information governance requirements and issues across all levels of the College.
 - To inform and advise about the necessary obligations that should be undertaken to comply with data protection legislation and all other applicable laws. This includes delivering training on data protection legislation and all other applicable laws.
 - To advise and monitor compliance with data protection legislation and all other applicable laws by conducting internal audits.
 - To advise and assist in the completion of data protection impact assessments (DPIA).
 - Continuously develop expertise on data protection sufficient to fulfil the role effectively.
 - To maintain current and accurate registration with the Information Commissioner's Office (ICO).
 - To be the first point of contact for the ICO and data subjects.
 - To be the initial contact for the investigation of data breaches, and, where required, for reporting data breaches to the ICO.
 - Seek the advice of the ICO or lawyers where there is uncertainty around a data protection matter.
 - Carry out responses to requests made by data subjects per their rights.
 - Consider the risk associated with processing operations, considering the nature, scope, context and purposes of processing when approving processing activities and data protection impact assessments.
 - Maintain the Records of Processing Activities as required by Article 30 of the UK GDPR to document regular processing activities.

- Per the above, the DPO is authorised to request and access any information that falls within the scope of their responsibilities.

21.2 Senior Leadership Team

- The following duties align with the responsibilities and remit of managers who form the Senior Leadership Team:
 - Encouraging data protection best practices.
 - Maintaining oversight of data protection within their respective service areas to ensure compliance with legislation in day-to-day activities.
 - Working with the DPO to ensure any necessary compliance measures identified are implemented within their respective service.

21.3 Head of IT Services

- The following duties align with the responsibilities and remit of the above postholder:
 - To ensure that appropriate and adequate technical measures are in place to safeguard the security of data.

- To advise and recommend additional requirements and developments that can be implemented to enhance data security and processes.
- To maintain awareness and understanding of current cybersecurity threats.

21.4 Head of Management Information Systems (MIS)

- The following duties align with the responsibilities and remit of the above postholder:
 - To maintain oversight of personal data processed about students. This includes admissions, examinations and academic performance data.
 - To work with the DPO to ensure the security and integrity of students' data processed within the MIS system.
 - To work with the DPO to ensure that the College responds to changes in legislation that will impact students' data.

21.5 Director of Human Resources (HR)

- The following duties align with the responsibilities and remit of the above postholder:
 - To maintain oversight of personal data processed about employees, which relates to the functions carried out by Human Resources.
 - To work with the DPO to ensure the security and integrity of the personal data processed about employees, which relates to the functions carried out by Human Resources.
 - To work with the DPO to ensure that the College responds to changes in legislation that will impact employees' data.
 - To ensure that the College provides a mechanism for employees to complete mandatory data protection training regularly.