DATA PROTECTION POLICY

Approval date:	**10th May 2018**
Approved by:	**Resources Committee**
Responsible Manager:	Executive Director Resources
Next Review	May 2020

Data Protection Policy - Preston's College

1. Introduction

1.1. This document outlines the steps which all members of Preston's College ("the College") must take to ensure that the College complies with the General Data Protection Regulations (GDPR) and supplementary enacting Data Protection legislation.

1.2. The College is committed to being transparent about how it collects and processes the personal data of its learners, employees, visitors and other stakeholders to meet its data protection obligations. This policy sets out the College's commitment to data protection, and individual rights and obligations in relation to personal data.

1.3. All members of the College have a duty to ensure compliance with the GDPR.

1.4. This policy applies to all personal and special category data that is held and processed by the College. The GDPR are technologically neutral, so this policy covers all manual records and data held electronically.

Definitions

"Personal data" is any information that relates to an individual who can be identified from that information.

"Special categories of personal data" means information about an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life or sexual orientation and biometric data.

"Processing" is any use that is made of data, including collecting, storing, amending, disclosing or destroying it.

2. Scope of this Policy

2.1. This policy applies to all staff, learners, apprentices and volunteer workers. It also applies to the following when they are acting on behalf of the College; Governors, employers of apprentices, contractors, subcontractors and any other third party.

3. Status of this Policy

3.1. This policy does not form part of the formal contract of employment for staff, but it is a condition of employment that employees will abide by the rules and policies made by the College. Any failure to follow this policy can therefore result in disciplinary proceedings or criminal prosecution for serious breaches.

4. Principles of the General Data Protection Regulations

4.1. The GDPR are in place to protect individuals by regulating the way in which the College collects, retains and uses personal data. Storing and processing data is governed by specific principles which state that the College shall:

4.1.1. process personal data lawfully, fairly and in a transparent manner;

4.1.2. collect personal data only for specified, explicit and legitimate purposes;

4.1.3. process personal data only where it is adequate, relevant and limited to what is necessary for the purposes of processing;

4.1.4. keep accurate personal data and take all reasonable steps to ensure that inaccurate personal data is rectified or deleted without delay;

4.1.5. keep personal data only for the period necessary for processing;

4.1.6. adopt appropriate measures to make sure that personal data is secure, and protected; against unauthorised or unlawful processing, and accidental loss, destruction or damage;

4.1.7. implement organisational and technical measures to ensure and be able to demonstrate that processing is performed in accordance with the regulations.

5. College Policy Statement

5.1. Preston's College will:

5.1.1. Comply with the General Data Protection Regulations;

5.1.2. Follow the relevant conditions for the lawful, fair and transparent processing of personal data;

5.1.3. Tell individuals the reasons for processing their personal data, how it uses such data and the legal basis for processing in its privacy notices. It will not process personal data of individuals for other reasons;

5.1.4. Provide information to staff, learners, employers, visitors and the general public on their rights under the GDPR;

5.1.5. Hold only the minimum personal data necessary to carry out the College's functions;

5.1.6. Make every effort to ensure the accuracy of the information held and ensure that where records include opinions and/or intentions, these are carefully and professionally expressed;

5.1.7. Update data promptly if an individual advises that their information has changed or is inaccurate;

5.1.8. Ensure that data which is no longer required or has reached it legal retention limit (as outlined in the College's Document Retention Schedule) is securely destroyed;

5.1.9. Advise individuals of the periods for which the College holds personal data. The retention period will be contained in all privacy notices;

5.1.10. Ensure that all College policies and processes comply with the GDPR and any new policies and procedures are privacy impact assessed and have individual's privacy at their core;

5.1.11. Periodically review and extend existing security measures to ensure these include all records containing personal information and continue to be effective in preventing the unauthorised or unlawful processing, or disclosure, accidental loss, alteration, damage and destruction of data and, consider adopting further safeguards, including for example, the use of encryption to secure e-mail attachments and privacy of internet communication;

5.1.12. Use personal data for the direct marketing of goods or services in circumstances where individuals have opted to receive it;

5.1.13. Only use wholly automated decision making processes where this is necessary;

5.1.14. Ensure all requests from individuals to access their personal data are dealt with as quickly as possible and at the latest within one month of receipt of the request;

5.1.15. Keep a record of its processing activities in respect of personal data being transferred to a third party, in accordance with the requirements of the General Data Protection Regulations.

6. The Data Protection Officer

6.1. The Designated Data Protection Officer (DPO) for Preston's College is the Head of MIS, ICT & Data Services, who is responsible for ensuring that the College is registered with the Information Commissioner's Office and that appropriate policies and procedures are in place. The Data Protection Officer will also ensure that procedures and processes are in place for dealing with data breaches, document retention, data security, subject access and freedom of information requests and will be the lead at any Information Commissioners Office (ICO) inspection.

6.2. To fully comply with the GDPR, the College has also two Designated Deputy Data Protection Officers; the Head of Human Resources and Head of Learner Support. The deputy will cover any periods whilst the Data Protection Officer is absent from work and investigate any breaches should there be any conflicts of interest.

6.3. The College as a corporate body is the Data Controller under the GDPR, and the Governors are therefore ultimately responsible for implementation. However, the Designated Data Protection Officers will deal with day to day matters. Any member of staff, student or other individual who considers that the Policy has not been followed in respect of personal data about himself or herself should raise the matter with the Data Protection Officer.

6.4. The executive GDPR lead is the Executive Director Resources. The Executive GDPR lead's main responsibilities are to chair the GDPR steering group and review any appeals to subject access or freedom of information requests.

6.5. Curriculum and support departments will themselves have designated staff, usually the Head of Department or School, who will provide the Designated Data Protection Officer with details of the data held in their departments, which will form part of the College Information Asset Register.

7. Responsibilities of Staff

7.1. All staff are responsible for:

7.1.1. Checking that any information that they provide to the College in connection with their employment is accurate and up to date.

7.1.2. Informing the College of any changes to information that they have provided, e.g. changes of address, either at the time of appointment or subsequently. The College cannot be held responsible for any errors unless the staff member has informed the College of such changes. Most changes to staff personal details can be made by individuals themselves via iTrent Self Service module. Alternatively, staff can inform HR directly.

7.2. If and when, as part of their responsibilities, staff collect information about other people (e.g. about a student's course work, opinions about ability, references to other academic institutions or details of personal circumstances), they must comply with this policy and the guidelines for staff set out in the College's GDPR Code of Practice.

8. Student Obligations

8.1. Students must ensure that all personal data provided to the College is accurate and up to date. They must ensure that changes of address and contact details are provided to the College via the Student portal or at the Learner Services desk.

8.2. Students who may from time to time process personal data as part of their studies (e.g. pictures of other students or staff) must notify their tutor, who should inform the Data Protection Officer, and must comply with the guidelines for data collection and security as set out in the College's GDPR Code of Practice.

8.3. Students are not permitted to upload images of staff to social media accounts, as this would be a breach of privacy and may result in disciplinary action.

9. Training

9.1. Governors and employees will be trained to an appropriate level in the use and control of personal data and guidance will be issued to Governors and employees explaining their rights and responsibilities under the Act, including the requirement to comply with this policy, the Code of Practice and any other relevant procedures, to ensure best practice is followed in all its information handling processes.

9.2. The College will provide training to all individuals about their data protection responsibilities as part of the induction process and at regular intervals thereafter.

9.3. The GDPR will be a mandatory training module for all staff and successful completion of the test will be a requirement of their employment.

9.4. Individuals whose roles require regular access to special category data, or who are responsible for implementing this policy or responding to subject access requests under this policy, will receive additional training to help them understand their duties and how to comply with them.

9.5. Staff and students will be provided with information outlining what data is held about them and their rights under GDPR. For learners this will be included in privacy notices and the student handbook. Staff will receive a new GDPR compliant employee privacy notice.

10. Data Security

10.1. The College takes the security of all personal data seriously. The College has internal policies and controls in place to protect personal data against loss, accidental destruction, misuse or disclosure, and to ensure that data is not accessed, except by employees in the proper performance of their duties.

10.2. All staff are responsible for ensuring that:

10.2.1. Any personal data that they hold is kept securely;

10.2.2. Personal information is not disclosed either orally, in writing or digitally or by any other means, accidentally or otherwise, to any unauthorised third party;

10.2.3. Staff should note that unauthorised disclosure will usually be a disciplinary matter, and may be considered gross misconduct in some cases (see Disciplinary Policy for further details);

10.2.4. Personal information, whether electronic or paper based, should be stored securely and in keeping with College procedures for document retention. Information should only be removed from its storage location when operationally necessary and with appropriate security measures in place;

10.2.5. If personal data is computerised, it must be encrypted or password protected on a device that is regularly backed up to the College network.

10.3. The College aims to minimise the storage of, and, access to personal data on removable media, such as laptops, external hard drives, flash drives and USB pens which may be lost or stolen. The requirements of 11.2.5 apply to all occasions where mobile devices or portable storage is used. Permission to store personal data on portable and removable media, must be given by the Data Protection Officer. A record of all decisions will be maintained.

10.4. Staff with mobile technology provided by the College must adhere to the Mobile Device Security Guide and Code of Practice.

10.5. Special Category data will not be permitted on mobile technology, except in extreme circumstances and with explicit permission from the Designated Data Protection Officer.

10.6. Where the College engages third parties to process personal data on its behalf (e.g. subcontractors) such parties, do so on the basis of written instructions, are under a duty of confidentiality and are obliged to implement appropriate technical and organisational measures to ensure the security of data.

10.7. Further guidance on data security is given in the College's GDPR Code of Practice.

11. IT Systems and Security under GDPR

11.1. Even though the General Data Protection Regulations are technologically neutral, they have significant implications for IT systems and cyber security. The College is required to provide 'appropriate technical and organisational measures', to ensure personal data is stored securely.

11.2. Individuals have the right to reasonably anticipate that their data will be stored securely and the College has safeguards in place to protect from external and internal hacks or malicious attacks.

11.3. The College has an Acceptable Use Policy and Information Security Policy which provide a framework for best operational practice, to minimise risk and respond effectively to new IT security threats and vulnerabilities as they emerge.

11.4. Periodic risk assessments, audits, health checks and penetration testing are undertaken to assess the IT security controls in place and ensure they provide a high level of protection against cybersecurity threats.

11.5. The College provides anti-virus software to all PCs connected to the College network and this is licensed for use on staff and student home computers, to reduce the transfer of malicious software or digital infections.

11.6. The College uses Microsoft Active Directory as the primary source of identification, for staff and students, for the majority of systems. The use of Active Directory provides a single sign-on solution for services provided by the College. This also ensures access to these systems can be removed in one place, reducing the risk of data breaches should a staff member leave the organisation.

11.7. The College provides separate domains/networks for staff, students and visitors, to provide logical segregation of services. Restrictions are in place to prevent direct access from student computers to data held on the staff network and core personal data systems (EBS, iTrent, ProMonitor etc).

11.8. Access to staff and student network services requires a unique user login, which is supplied at the point of employment or following enrolment. All new account requests or cancellations for the staff network are validated by Human Resources. Student accounts are created following enrolment and are given an expiry date based on a learner's course end date.

11.9. The College operates password policies which require staff users to change their password every 60 days and they unable to change it to a password previously used.

11.10. In order to comply with the GDPR principle of keeping the minimum amount of data, quotas are used to encourage storage resources are not misused or unnecessary data kept for longer than the retention periods.

11.11. To protect against cybersecurity threats and ensure the data stored is secure, the College has an array of security measures in place, that provide a multi-layered approach to protection; firewall, e-mail filtering, spyware, virus protection, web filtering, patching, encryption, rights management, third party 24 hour network monitoring (JISC), enhanced desktop security policy, zero-day solutions and network restrictions.

11.12. Further guidance and details on the IT security measures, infrastructure and policies in place to provide the College with the appropriate level of protection required for GDPR can be found in the Information Security Policy.

12. Cloud Storage

12.1. There are an increasing number of services offering 'cloud storage' where users can upload documents, photos, videos and other files to share or act as a backup. These files can then be accessed from any location or device. Storing information in the 'cloud' means you are storing data on servers external to the College that are controlled by someone else, many of which are outside the European Economic Area.

12.2. The College has one of its core data system in the cloud; OneFile (apprenticeship e-portfolio). The data is stored in Birmingham and backup in the UK, under strict contractual agreement, to ensure compliance with GDPR.

12.3. The College has other cloud servers/services (Azure), which are used for non-personal data.

12.4. The only cloud storage that staff are authorised to use is Office365 for document storage and sharing documents. Office365 is also used by learners for document storage and for cloud based e-mail.

12.5. All other cloud storage solutions (e.g. Dropbox, Barracuda, livedrive etc.) to store personal data are not permitted under this policy. The use of any alternative cloud storage solutions needs approval from the Designated Data Protection Officer, following due diligence on the storage provider's terms and conditions and privacy notices. Most cloud storage providers servers are based outside the EEA, so the College would need to ensure the conditions of International Data Transfers in this policy are met.

13. International Data Transfers

13.1. The College will only transfer data to a third country or territory outside the European Economic Area, or an international organisation where the transfer is:

13.1.1. made with the individuals informed consent;

13.1.2. necessary for the performance of a contract between the individual and the College or for pre-contractual steps taken at the individual's request;

13.1.3. necessary for important reasons of public interest;

13.1.4. necessary for the establishment, exercise or defence of legal claims;

13.1.5. necessary to protect the vital interests of the data subject, where the individual is physically or legally incapable of giving consent.

14. Rights to Access Information

14.1. All staff and students, as data subjects, have a number of rights in relation to their personal data. Individuals have the right to make a subject access request. If an individual makes a subject access request, the College will provide them with the following:

14.1.1. whether or not their data has been processed and if so why, the categories of personal data concerned and the source of the data if it is not collected from the individual;

14.1.2. to whom their data has or may be disclosed, including to recipients located outside the European Economic Area (EEA) and the safeguards that apply to such transfers;

14.1.3. for how long their personal data will be stored (or how that period is decided);

14.1.4. their rights to rectification or erasure of data, or to restrict or object to processing;

14.1.5. their right to complain to the Information Commissioner if they think the College has failed to comply with his/her data protection rights; and

14.1.6. whether or not the College carries out automated decision-making and the logic involved in any such decision-making.

14.2. The College will also provide the individual with a copy of the personal data undergoing processing. This will normally be in electronic form if the individual has made a request electronically, unless he/she agrees otherwise.

14.3. If the individual requires additional copies, the College will charge a fee, which will be based on the administrative cost to the College of providing the additional copies.

14.4. To make a subject access request, the individual should send the request either by e-mail to gdpr@preston.ac.uk or in writing to the Data Protection Officer. In some cases, the College may need to ask for proof of identification before the request can be processed. The College will inform the individual if it needs to verify his/her identity and the documents it requires to do so.

14.5. The College will normally respond to a request within a period of one month from the date it is received. In some cases, such as where the College processes large amounts of the individual's data, it may respond within three months of the date the request is received. The College will write to the individual within one month of receiving the original request to tell him/her if this is the case.

14.6. To prevent delay by having to ask data subjects for further information and, to ensure these are processed within the necessary time scale, all requests from data subjects must:

14.6.1. be made in writing;

14.6.2. be accompanied by adequate proof of the identity of the data subject and, where applicable the written authorisation of the data subject if the request is being made on their behalf by a legal or lawfully appointed representative or, authorised agent;

14.6.3. specify the information required;

14.6.4. give adequate information to enable the requested data to be located;

14.7. If a subject access request is manifestly unfounded, unauthorised or excessive, the College is not obliged to comply with it. Alternatively, the College can agree to respond but will charge a fee, which will be based on the administrative cost of responding to the request. A subject access request is likely to be manifestly unfounded or excessive where it repeats a request to which the College has already responded. If an individual submits a request that is unfounded or excessive, the College will notify him/her that this is the case and whether or not it will respond to it.

15. Other rights of individuals

15.1. Individuals have a number of other rights in relation to their personal data. They can require the College to:

15.1.1. rectify inaccurate data;

15.1.2. stop processing or erase data that is no longer necessary for the purposes of processing;

15.1.3. stop processing or erase data if the individual's interests override the College's legitimate grounds for processing data (where the College relies on its legitimate interests as a reason for processing data);

15.1.4. stop processing or erase data if processing is unlawful; and

15.1.5. stop processing data for a period if data is inaccurate or if there is a dispute about whether or not the individual's interests override the College's legitimate grounds for processing data.

15.2. To ask the College to take any of the steps in 12.1, the individual should send the request to gdpr@preston.ac.uk or use the link on the desktop app or student portal to report inaccurate or changes to data.

16. Individual Responsibilities

16.1. Individuals are responsible for helping the College keep their personal data up to date. Individuals should let the College know if data provided to the College changes, for example if an individual moves house or changes his/her bank details.

16.2. Individuals may have access to the personal data of other colleagues, learners, employers, visitors and other stakeholders in the course of their employment, contract, volunteer period, study or apprenticeship. Where this is the case, the College relies on individuals to help meet its data protection obligations.

16.3. Individuals who have access to personal data are required:

16.3.1. to access only data that they have authority to access and only for authorised purposes;

16.3.2. not to disclose data except to individuals (whether inside or outside the College) who have appropriate authorisation;

16.3.3. to keep data secure (for example by complying with rules on access to premises, computer access, including password protection, and secure file storage and destruction);

16.3.4. not to remove personal data, or devices containing or that can be used to access personal data, from the College's premises without adopting appropriate security measures (such as encryption or password protection) to secure the data and the device; and

16.3.5. not to store personal data on local drives or on personal devices that are used for work purposes.

16.4. Further details about the College's security procedures can be found in its Information Security Guide.

16.5. Failing to observe these requirements may amount to a disciplinary offence, which will be dealt with under the College's disciplinary procedure. Significant or deliberate breaches of this policy, such as accessing employee or learner data without authorisation or a legitimate reason to do so, may constitute gross misconduct and could lead to dismissal or criminal prosecution.

17. CCTV

17.1. The College will follow the guidance in the Information Commission's Code of Practice for users of CCTV and similar surveillance equipment monitoring spaces to which the public, learners and employees have access.

17.2. Areas where CCTV is in operation will have clear signage so people are aware they are being recorded.

17.3. The College retains CCTV images for no longer than 30 days, unless the images are being used for an investigation or have been requested via a subject access request.

18. Monitoring of Communications

18.1. The College reserves the right to monitor telephone calls, e-mails and Internet access on its own networks, in compliance with the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, Privacy and Electronic Communications Regulations, GDPR, Human Rights Act 1998 and any other relevant legislation. This will be subject to the Information Commissioners Code of Practice on Employer/Employee Relationships.

18.2. The College does not monitor, inspect or disclose electronic communications or documents, without consent, unless one or more of the following circumstances is identified:
  18.2.1. Required by and consistent with law;
  18.2.2. Breach of legislation or Preston's College policy;
  18.2.3. Compelling or emergency circumstances;
  18.2.4. Time dependent, business critical need.
18.3. Any monitoring or access must be risk assessed and signed off by both the Data Protection Officer and Principal and Chief Executive.

19. **Achievement Data**

19.1. During the course of their studies, students will routinely be provided with information about their results for both coursework and examinations. Assessed coursework and exam grades are classed as personal data under the General Data Protection Regulations, so should be kept private and not published on notice boards or announced in class in front of other learners.

19.2. Exam scripts themselves are exempted from the subject access rules and copies will not ordinarily be given to a student who makes a subject access request. The College does not hold copies of exam scripts, as these are sent directly to the awarding bodies, following an exam. If a student wishes to gain access to their exams scripts they will need to make an application to the appropriate awarding body via the Exams Office. The procedures set out in the JCQ publication Post Results Services, which is reviewed annually, will be adhered to.

20. Subject Consent

20.1. In many cases, the College can only process personal data with the consent of the individual. In some cases, if the data is sensitive, as defined in the General Data Protection Regulations, express consent must be obtained. Agreement to the College processing some specified classes of personal data is a condition of acceptance of a student onto any course, and a condition of employment for staff. This includes information about previous criminal convictions.

20.2. Some jobs or courses will bring the applicants into contact with children, including young people between the ages of 14 and 18. The College has a duty under the Children Act 1989 and other enactments to ensure that staff are suitable for the job, and students for the courses offered. The College also has a duty of care to all staff and students and must therefore make sure that employees and those who use College facilities do not pose a threat or danger to other users.

20.3. The College may also ask for information about particular health needs, such as allergies to particular forms of medication, or any medical condition such as asthma or diabetes. The College will only use this information in the protection of the health and safety of the individual, but will need consent to process this data in the event of a medical emergency, for example.

20.4. Therefore, the application forms that all prospective staff and students are required to complete will include a section requiring consent to process the applicant's special category and personal data. A refusal to sign such a form will prevent the application from being processed and withholding information, may result in disciplinary action.

21. Impact Assessments

21.1. Some of the processing that the College carries out may result in risks to privacy. Where processing would result in a high risk to individual's rights and freedoms, the College will carry out a data protection impact assessment to determine the necessity and proportionality of processing. This will include considering the purposes for which the activity is carried out, the risks for individuals and the measures that can be put in place to mitigate those risks.

21.2. All data protection impact assessments will be reviewed and risk assessed by the GDPR steering group.

22. Data breaches

22.1. If the College discovers that there has been a breach of personal data that poses a risk to the rights and freedoms of individuals, it will report it to the Information Commissioner within 72 hours of discovery. The College will record all data breaches regardless of their effect.

22.2. If the breach is likely to result in a high risk to the rights and freedoms of individuals, it will tell affected individuals that there has been a breach and provide them with information about its likely consequences and the mitigation measures it has taken.

23. Processing Special Category Data

23.1. Sometimes it is necessary to possess information about a person's health, criminal convictions, religious beliefs, bio-metric data, ethnicity, and trade union membership. This may be to ensure that the College is a safe place for everyone, or to operate other College policies, such as the sick pay policy or the Equality and Diversity policy. The College also has a contractual or legal duty to collect a variety of special category data on behalf of the Funding Agencies. An offer of employment or a course place may be withdrawn if an individual refuses to consent to the collection or processing, without good reason.

23.2. Special Category data will not be permitted on mobile technology, except in extreme circumstances and with explicit permission from the Designated Data Protection Officer.

24. Retention of Data

24.1. The College has a duty to retain some staff and student personal data for a period of time following their departure from the College, mainly for legal reasons, but also for other purposes such as being able to provide references and academic transcripts, or for financial reasons, for example relating to pensions and taxation. Different categories of data will be retained for different periods of time. The exact details of retention periods and purposes are set out in the College Document Retention Schedule.

25. Publication of College Information

25.1. The names of Senior Managers and Governors of the College or any other personal data relating to senior employees or Governors will be published in the annual Operating and Financial Review, Financial Statements and on the public Web site when any statute or law requires such data to be made public.

25.2. Certain items of information relating to College staff will be made available via searchable directories on the public website, in order to meet the legitimate needs of researchers, visitors and enquirers seeking to make contact with appropriate staff. However, it is not expected that the names of staff who are not 'Heads of' will be in the public domain, without their consent.

26. Compliance

26.1. Compliance with the General Data Protection Rules is the responsibility of all members of the College. Any deliberate breach of the data protection policy may lead to disciplinary action being taken or to access to College facilities being withdrawn, or even to a criminal prosecution. Any questions or concerns about the interpretation or operation of this policy should be directed to the Designated Data Protection Officer.