Data Protection Policy

Author: Director of HR & Culture

Equality Assessment: Director of HR & Culture **Date:** August 2025

Version and Date		Actions/Notes
1.0	August 2024	N/A
2.0	August 2025	Added the reference to the Data (Use and Access) Act 2025: data protection and privacy changes (Gov.uk, published 27 June 2025) Section 14 – 3.4 additional info Subject Access Requests will normally be complied with within one calendar month of receipt of a request. It includes a "stop the clock" rule, allowing organisations to pause the response time if they need more information from the requester. Once the information is received, the response time continues. Section 17 – The College allows for individuals to request human intervention into any significant automated decision making. Section 21 – added for to refer to AI Policy

Approved by SMT:	August 2025
Approved by Corporation:	**TBC**
Date of Next Review:	August 2026
Related policies or procedures or parent policy if applicable:	Data Breach Policy & Procedure Online Safety Policy Data Protection Policy IT Acceptable Use Policy - Staff IT Acceptable Use Policy - Student Information Security Policy AI Policy
Groups/bodies consulted in the development of the policy:	General Data Protection Regulation (GDPR) 2018 & Data Protection Act 2018 Freedom of Information Act 2000 Privacy and Electronic Communications Regulations (PECR) Data (Use and Access) Act 2025: data protection and privacy changes (Gov.uk, published 27 June 2025)
To be published on College Website:	YES
To be published on Student Hub:	NO

1. INTRODUCTION

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.

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, contractors and volunteers, 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.

The College has implemented this Data Protection Policy to ensure all College Personnel 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.

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

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

2. ABOUT THIS POLICY

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

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

3. DEFINITIONS

3.1. **College** – Macclesfield College

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

3.3. **Controller** - Any entity (e.g. company, organisation, 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.

3.4. **Data Protection Laws** - The General Data Protection Regulation (Regulation (EU) 2016/679) and 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.

3.5. **Data Protection Officer -** Our Data **Protection** Officer is The Director of Human Resources & Culture, and can be contacted at: dpo@macclesfield.ac.uk

3.6. **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.

3.7. **ICO** - the Information **Commissioner's** Office, the UK's data protection regulator.

3.8. **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.

3.9. **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.

3.10. **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. COLLEGE PERSONNEL'S GENERAL OBLIGATIONS

This policy does not form part of the formal contract of employment, but it is a condition of employment that all College Personnel will abide by the rules and policies of the College. Any failure to not follow the policy can therefore result in disciplinary proceedings being instigated with a possible outcome including dismissal.

RESPONSIBILTIES

4.1. All staff are responsible for:

- Checking that any information that they provide to Macclesfield College in connection with their employment is accurate and up to date;
- Informing Macclesfield College of any changes to information, which they have provided i.e. changes of address; this can be done on the College CipHr site;
- Informing Macclesfield College of any errors or changes. Macclesfield College cannot be held responsible for any errors unless the staff member has informed the College of them;
- Ensuring that personal data which they hold on students is kept securely (locked filing cabinet/drawer/on the network);
- Not disclosing any personal data which they hold on students (orally, in writing or electronically) to an unauthorised third party without the prior consent of the Data Protection Officer or a member of the Executive team;
- Ensuring that personal data which they hold on students is not stored on any removable media (e.g. USB stick);
- Ensuring that any data approved for disclosure and sent electronically must be encrypted and the encryption key sent separately;
- Inform the Data Protection Officer of any proposed new uses of personal data;
- Comply with the College's IT policy in relation to security, ensuring that if and when, as part of their responsibilities, staff collect information about other people, (i.e. about students' course work, opinions about ability, references to other academic institutions, or details of personal circumstances), they must comply with the above guidelines;
- Destroying personal data according to the College's Retention of Personal Data Policy.

4.2. Students are responsible for:

- Checking that the information they provide to the College in connection with their enrolment is accurate and up to date;
- Informing the College of any changes to the information they provide, such as, change of address, emergency contact details;
- Not seeking to gain unauthorised access to personal information;
- Complying with all College policies regarding the use of IT facilities. Managers are responsible for:
- Ensuring they are satisfied with the legality of holding and using the information collected by staff in their area;
- Ensuring they keep the College data documentation controller spreadsheet up to date based on their areas of responsibility;
- Ensuring that the use of personal data complies with all appropriate college policies;
- Ensuring that relevant staff they manage, undertake the Data Protection training;

- Referring any non-routine requests for disclosure, requests for subject access and requests to cease processing to the Data Protection Officer;
- Raise any concerns, notify any breaches or errors, and report anything suspicious or contradictory to this policy or our legal obligations without delay;
- Checking and approving with third parties that handle the company's data any contracts or agreement regarding data processing.

4.3. The IT Systems Team are responsible for:

Whilst all staff and users of personal data have some responsibility for the security of data, Computer Services and Information Systems staff have an important role in ensuring the security of computerised data. In particular, they will:

- Be responsible for advising the College on the state of technological development with regard to IT security;
- Provide secure methods of transferring authorised personal data outside the College
- Back up data on the College's IT systems and have disaster recovery procedures in place and tested;
- Implement virus detection and hacking preventative measures;
- Through liaison with the appropriate manager, ensure that the College's business systems are secure and appropriate restrictions on access are in place so that individuals only have access to personal data in which they have a legitimate business interest;
- Require the use of passwords and ensure they are changed regularly;
- Produce and update policies for the use of College IT facilities including email, intranet, and internet;
- Investigate breaches of IT security;
- Ensure that data is deleted according to the College's Retention of Personal Data Policy.

4.4. The Marketing Team are responsible for:

- Approving data protection statements attached to emails and other marketing copy;
- Addressing data protection queries from clients, target audiences or media outlets.

4.5. The Human Resources Team will:

- Ensure that the College's Employment Practices are consistent with the Employment Codes of Practice;
- Ensure that Data Protection obligations are reflected in the College's Disciplinary Procedures and contracts of employment;
- Ensure that all staff are aware of the types of personal information that the College will process on them and ask staff to check this information as required;
- Ensure that all obligations outlined within the Disclosure and Barring Service (DBS) Code of Practice published under section122 of the Police Act 1997 are adhered to. Full details of the CRB Code of Practice can be found at http://www.gov.uk/government/organisations/disclosure-and-barring-service
- Provide advice to managers and others on the application of the DBS Code of Practice;

- Destroy personal data according to the College's Retention of Personal Data Policy.

4.6. The College's Data Protection Officer will:

- Maintain the College's Data Protection registration, liaise with the Information Commissioner's Office and the College's legal advisers as required;
- Make recommendations to the College Leadership Team (ELT) regarding Data Protection/GDPR Policy and good practice;
- Provide general guidance and advice and dissemination of information regarding Data Protection;
- Deal with subject access requests and co-ordinate responses;
- Co-ordinate and advise on all non-routine requests for disclosure of personal information;
- Monitor and report on data protection requests;
- Deal with any data breaches/complaints.

4.7. All college personnel are responsible for helping the College keep their personal data up to date. Individuals should notify the College of any changes in their data i.e. if a staff member moves house, or changes their bank details. In all circumstances the CIPHR system should be updated.

4.8. College personnel must ensure that they keep confidential all personal data that they collect, store, use and come into contact with during the performance of their duties i.e. where they have access to the personal data of other individuals such as students.

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

- Access only data that they have authority to access and only for authorised purposes;
- Not to disclose data except to individuals (whether inside the College, or outside the organisation) who have appropriate authorisation;
- To keep data secure (for example by complying with rules on access to premises, password protection);
- Not to remove personal data, or devices containing, or that can be used to access personal data, from the College without applying the appropriate security measures (such as encryption) to secure the data and the device;
- Not to store personal data on local drives, or on personal devices that are used for work purposes, and
- Report data breaches of which they become aware to the Data Protection Officer immediately.

Any member of staff, who considers that the policy has not been followed in respect of personal data about themselves, should raise the matter with the Data Protection Officer initially. If the matter is not resolved, it should be raised as a formal grievance.

5. DATA PROTECTION PRINCIPLES

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

- Processed **lawfully, fairly and in a transparent manner;**
- Collected for **specified, explicit and legitimate purposes** and not further processed in a manner that is incompatible with those purposes;
- **Adequate, relevant, and limited** to what is necessary for the purposes for which it is being processed;
- **Accurate** and kept up to date, meaning that every reasonable step must be taken to ensure that Personal Data that is inaccurate is erased or rectified as soon as possible;
- **Kept for no longer than is necessary** for the purposes for which it is being processed; and
- Processed in a manner that ensures appropriate **security and integrity** 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. These principles are considered in more detail in the remainder of this Policy.

5.3. In addition to complying with the above requirements the College also has to demonstrate in writing that it complies with them. The College has a number of policies and procedures in place, including this Policy and the documentation referred to in it, to ensure that the College can demonstrate its compliance.

6. LAWFUL USE OF PERSONAL DATA

6.1. In order to collect and/or use personal data lawfully the College needs to be able to show that its use meets one of a number of legal grounds. Please click here to see the detailed grounds [https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing].

6.2. In addition, when the College collects and/or uses special categories of personal data, the College has to show that one of a number of additional conditions is met. Please click here to see the detailed additional conditions [https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/special-category-data].

6.3. The College has carefully assessed how it uses personal data and how it complies with the obligations set out in paragraphs 6.1 and 6.2. If the College changes how it uses personal data, the College needs to update this record and may also need to notify Individuals about the change. If college personnel therefore intend to change how they use personal data at any point they must notify the Data Protection Officer who will decide whether their intended use requires amendments to be made and any other controls which need to apply.

7. TRANSPARENT PROCESSING - PRIVACY POLICY

7.1. Where the College collects personal data directly from individuals it will comply with the rights of the data subject including the right to inform them about how the

College uses their personal data. This is in a privacy policy. The College has adopted the following privacy notices:

- Applicant Privacy Policy
- Employee Privacy Statement

7.2. If the College receives personal data about an Individual from other sources, the College will provide the individual with a privacy policy 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.

7.3. If the College changes how it uses personal data, the College may need to notify individuals about the change. If college personnel therefore intend to change how they use personal data, please notify the Data Protection Officer who will decide whether the College Personnel's intended use requires amendments to be made to the privacy notices and any other controls which need to apply.

8. DATA QUALITY - ENSURING THE USE OF ACCURATE, UP TO DATE AND RELEVANT PERSONAL DATA

8.1. 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 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.

8.2. All College Personnel 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.

8.3. All College Personnel 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 College Personnel to independently check the Personal Data obtained.

8.4. In order to maintain the quality of Personal Data, all College Personnel 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).

8.5. 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.

9. RETENTION OF PERSONAL DATA

9.1. 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.

9.2. 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.

9.3. All Staff have a responsibility to comply with the College Data Retention Policy and the retention period defined with in it ensuring that personal data that has reached the end of its retention period is either destroyed, or anonymised. (*Data which has been anonymised so that identifying information has been removed from its content, may be kept by the College for an indefinite period).*

9.4. If College Personnel 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 College Personnel have any questions about this Policy or the College's Personal Data retention practices, they should contact the Data Protection Officer for guidance.

9.5. In circumstances where an individual submits a request for their personal data to be deleted, the College will take account of its Data Retention Policy to see if there are reasons why it may not be appropriate to comply with the request i.e. when it is necessary to retain the data due to a legal, statutory, regulatory, or security reason.

10. RECORD DISPOSAL

10.1. The College has robust processes in place to ensure that personal data is disposed in a way that protects the rights and privacy of data subjects (e.g. disposal via confidential waste, shredding), destruction of personal data must include all copies/backups.

Personal Data which will not be destroyed will be that pending an investigation, litigation, or audit, or being processed as part of an outstanding subject access request.

11. DATA SECURITY

11.1. 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.

11.2. All College Personnel are responsible for ensuring the personal data they process is managed and kept secure aligned with College Policy and not shared with any unauthorised party.

11.3. Personal Data must only be accessed by individuals who as a part of their responsibilities/association with the College need to use it. On all occasions

electronic data should be stored securely, password protected in alignment with College Procedures. Alternatively, hard paper copy must be stored in locked cabinets.

11.4. Processing of personal data off college premises should be undertaken in accordance with the policy and procedures.

12. DATA BREACH

12.1. 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 College Personnel must comply with the College's Data Breach Notification Policy.

12.2. 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.

12.3. 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.

12.4. Any data breaches must be reported using the form at Appendix 1 and sent to the College Data Protection Officer.

12.5. **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 College Personnel 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 ransomware, 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.

12.6. In circumstances, where an individual either suspects or discovers a personal data breach including unauthorised, or unlawful processing, accidental loss, destruction, or damage to personal data they have a responsibility to report it immediately in accordance with the College Data Breach Policy. The Data Protection Officer must also immediately be notified to enable the appropriate action to be initiated.

12.7. Where a data breach has occurred as a result of misconduct, or malicious intent it is considered to be an offence and, in such circumstances the College's Disciplinary Policy would be initiated and action being taken, access to college facilities being withdrawn, or even a criminal conviction.

13. APPOINTING CONTRACTORS WHO ACCESS THE COLLEGE'S PERSONAL DATA

13.1. 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.

13.2. One requirement of the Data Protection Act is that a Controller must only use Processors who meet the requirements of the Act 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.

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

13.4. 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.

13.5. The Data Protection Act 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 Data Protection Act, or other EU state data protection law.

13.6. 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.

14. INDIVIDUALS' RIGHTS

14.1. The College observes and comply with the rights of the data subject, including:

- The right of access (Subject Access Requests)
- The right to be informed (Data Privacy Notices)

(Data subject rights are not all 'absolute rights', the College may maintain the right to apply conditions, or exceptions, where it has a lawful basis to do so i.e. where the College has a legal obligation to process, or retain personal data.)

14.2. The different types of rights of individuals are reflected in this paragraph.

14.3. **Right of Access** - **Subject Access Requests**

Individuals have the right to ask the College to confirm what personal data they hold in relation to them and provide them with the data.

An **individual** wishing to exercise their right to request **access** to their personal data should submit their request in writing to the Data Protection Officer. dpo@macclesfield.ac.uk.

The College will verify the identity of the individual submitting the data subject access request. In circumstances where there are doubts about the identity of an individual making the request, further information will be sought. In such cases the individual's data subject request will only commence once the College has received the additional information requested is received and the data subject's identity verified.

Subject Access Requests will normally be complied with within one calendar month of receipt of a request. It includes a "stop the clock" rule, allowing organisations to pause the response time if they need more information from the requester. Once the information is received, the response time continues.

On occasion when responding to a complex subject access request, or a number of requests from an individual, it may be necessary to extend the original date of reply to the data subject request. In such circumstances the College will notify the individual within one month of receiving their request advising of the new date of reply, normally within a period of three months.

Where the College has received a subject access request which is broad, it will invite the data subject to provide further specific detail regarding the information, or processing activities to which the request relates.

Subject Access Requests are often made in the context of a dispute which means that it is crucial that they are handled appropriately to avoid a complaint being made to the ICO.

If a subject access request is manifestly unfounded, 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 considered manifestly unfounded or excessive where it repeats a request to which the College had already responded. If an individual submits a request that it is unfounded, or excessive, the College will notify him/her that this is the case and whether or not it will respond to it.

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

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

- The use of the Personal Data is no longer necessary;
- Their consent is withdrawn and there is no other legal ground for the processing;
- The individual objects to the processing and there are no overriding legitimate grounds for the processing;
- The Personal Data has been unlawfully processed; and
- The Personal Data has to be erased for compliance with a legal obligation.

In a marketing context, where Personal Data is collected and processed for direct marketing purposes, the individual has a right to object to processing at any time. Where the individual objects, the Personal Data must not be processed for such purposes.

14.5. **Right of Data Portability**

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

- The processing is based on consent or on a contract; and
- The processing is carried out by automated means

This right is not the same as subject access and is intended to give individuals a subset of their data.

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

Finally, individuals are also given the right to request that any Personal Data is rectified if inaccurate and to have use of their Personal Data restricted to particular purposes in certain circumstances.

14.7. The College will use all Personal Data in accordance with the rights given to Individuals under Data Protection Laws and will ensure that it allows Individuals to exercise their rights in accordance with the College's Rights of Individuals Policy and Rights of Individuals Procedure. Please familiarise yourself with these documents as they contain important obligations which College Personnel need to comply with in relation to the rights of Individuals over their Personal Data.

15. MARKETING AND CONSENT

15.1. The College will sometimes contact individuals to send them marketing or to promote the College. Where the College carries out any marketing, Data Protection Laws require that this is only done in a legally compliant manner. In most cases the College will only send marketing information to individuals who have expressly provided formally their consent. Records of consent will be retained by the College for marketing purposes for the duration that the data is needed. *The Data Protection Act defines 'consent as freely given, specific and informed.'*

15.2. The College will provide in each direct marketing communication a 'right to opt-out' of receiving marketing information they have previously consented to receive. In such circumstances, the College will action the request in a timeline of 30 days.

15.3. Separately, the College will from time-to-time contact individuals who have previously provided their consent to receive direct marketing from the College with an opportunity for them to update their details and reaffirm that they wish to continue to receiving promotional material from the College.

16. CCTV

16.1. The College Close Circuit Television complies with the laws relating to data protection, and includes the principles governing the processing of personal data.

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 decides about an Individual solely by automated means without any human involvement and the decision has legal or other significant effects.

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 College Personnel therefore wish to carry out any Automated Decision Making or Profiling College Personnel must inform the Data Protection Officer.

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

17.4. The College allows for individuals to request human intervention into any significant automated decision making.

18. DATA PROTECTION IMPACT ASSESSMENTS (DPIA)

18.1. A DPIA should be started as early as practical in the design of processing operations. 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.

18.2. 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. The ICO's standard DPIA template is available from www.ico.org.uk.

18.3. Where a DPIA reveals risks, which are not appropriately mitigated the Director of Finance and Estates must be consulted for initial consideration.

18.4. 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.

18.5. 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 (see definitions above) 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.

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

19. TRANSFERRING PERSONAL DATA TO A COUNTRY OUTSIDE THE EEA

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

19.2. So that the College can ensure it is compliant with Data Protection Laws College Personnel must not export Personal Data unless it has been approved by the Data Protection Officer and Executive Leadership Team.

19.3. College Personnel must not export any Personal Data outside the EEA without the approval of the Data Protection Officer and the Executive Leadership Team.

20. TRAINING

20.1. The College requires all new staff upon appointment to complete the Educare Data Protection Training e-certificated training course and staff to annually undergo Data Protection Training and the College's Cyber Security training.

20.2. All staff are required to complete mandatory refresher Data Protection & Cyber Security training annually, to complement any statutory, or best practice guidance and to undertake any other such data protection/information security training as required by the College.

21. AI Data Protection containing AI is documented in the College AI Policy

22. REVIEW AND MONITORING

22.1. The relevance, efficiency and effectiveness of this Data Protection Policy will be reviewed in line with the annual cycle of strategic management activities to facilitate continuous improvement. The results of the review process will be analysed and changes made to the policy where appropriate.