



Data Protection Policy

Document Control:

Version	V2
Document Created Date:	June 2023
Document Last Approval:	
Document Update History:	
Document Next Review:	June 2024
Document Approval Authority:	Senior Management Team (SMT)
Document Owner:	Vice Principal Information Services

TABLE OF CONTENTS

1. OVERVIEW	2
2. ABOUT THIS POLICY	2
3. DEFINITIONS	2
4. COLLEGE PERSONNEL'S GENERAL OBLIGATIONS.....	4
5. DATA PROTECTION PRINCIPLES	4
6. LAWFUL USE OF PERSONAL DATA.....	5
7. TRANSPARENT PROCESSING – PRIVACY NOTICES	5
8. DATA QUALITY – ENSURING THE USE OF ACCURATE, UP TO DATE AND RELEVANT PERSONAL DATA.....	6
9. PERSONAL DATA MUST NOT BE KEPT FOR LONGER THAN NEEDED.....	6
10. DATA SECURITY	7
11. DATA BREACH	7
12. APPOINTING CONTRACTORS WHO ACCESS THE COLLEGE'S PERSONAL DATA.....	7
13. INDIVIDUALS' RIGHTS	9
14. MARKETING AND CONSENT	10
15. AUTOMATED DECISION MAKING AND PROFILING.....	11
16. DATA PROTECTION IMPACT ASSESSMENTS (DPIA)	11
17. TRANSFERRING PERSONAL DATA TO A COUNTRY OUTSIDE THE EEA	12

1. OVERVIEW

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' applicants, 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.

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 our Data Protection Officer, who is responsible for ensuring the College's compliance with this Policy.

2. ABOUT THIS POLICY

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

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

3. DEFINITIONS

- 3.1. **College** – City of Portsmouth College.
- 3.2. **College Personnel** – Any College employee, governor, 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 Chris Caddamy – Vice Principal Information Services and can be contacted at: dpo@copc.ac.uk
- 3.6. **ICO** – the Information Commissioner’s Office, the UK’s data protection regulator.
- 3.7. **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.
- 3.8. **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.

- 3.9. **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.

- 3.10. **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

- 4.1. All College Personnel including governors must comply with this policy.
- 4.2. College Personnel must ensure that they keep confidential all Personal Data that they collect, store, use and come into contact with during the performance of their duties.
- 4.3. College Personnel must not release or disclose any Personal Data:
 - 4.3.1. outside the College; or
 - 4.3.2. inside the college to College Personnel not authorised to access the Personal Data, without specific authorisation from their manager or the Data Protection Officer; this includes by phone calls or in emails.
 - 4.3.3. College Personnel must take all steps to ensure there is no unauthorised access to Personal Data whether by other College Personnel who are not authorised to see such Personal Data or by people outside the College.

5. DATA PROTECTION PRINCIPLES

- 5.1. When using Personal Data, Data Protection Laws require that the College complies with the following principles. These principles require Personal Data to be:
 - 5.1.1. processed lawfully, fairly and in a transparent manner;
 - 5.1.2. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
 - 5.1.3. adequate, relevant and limited to what is necessary for the purposes for which it is being processed;
 - 5.1.4. 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;
 - 5.1.5. kept for no longer than is necessary for the purposes for which it is being processed; and
 - 5.1.6. 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. 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. The primary function of the College is that of education, either as a provider or in support of the providers. In order for the use of personal data to be lawful, the purpose should relate to:
- A legitimate and justified function of an educational establishment;
 - the articles of corporation or funding agreement for the establishment; and
 - meet a condition for processing established by Article 6 (and Articles 9 and 10 where necessary) of the GDPR.
- 6.2. 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>.
- 6.3. 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>.
- 6.4. 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 NOTICES

- 7.1. Where the College collects Personal Data directly from Individuals, the College will inform them about how the College uses their Personal Data. This is in a privacy notice. The College has adopted the following privacy notices:
- Privacy Notice for Students
 - Privacy Notice for Parents/Carers
 - Privacy Notice for Employers
- 7.2. 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.
- 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 (see paragraph 7 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.
- 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. PERSONAL DATA MUST NOT BE KEPT FOR LONGER THAN NEEDED

- 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. 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.

10. DATA SECURITY

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. DATA BREACH

11.1. 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. Please see paragraphs 11.2 and 11.3 for examples of what can be a Personal Data breach. Please familiarise yourself with it as it contains important obligations which College Personnel need to comply with in the event of Personal Data breaches.

11.2. 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.

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

11.3.1. **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.

11.3.2. **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.

11.3.3. **Integrity breach** - where there is an unauthorised or accidental alteration of Personal Data.

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

12.1. 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.

12.2. 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.

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

12.4. 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.

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

12.5.1. to only act on the written instructions of the Controller;

12.5.2. to not export Personal Data without the Controller's instruction;

12.5.3. to ensure staff are subject to confidentiality obligations;

12.5.4. to take appropriate security measures;

12.5.5. to only engage sub-processors with the prior consent (specific or general) of the Controller and under a written contract;

12.5.6. to keep the Personal Data secure and assist the Controller to do so;

12.5.7. to assist with the notification of Data Breaches and Data Protection Impact Assessments;

12.5.8. to assist with subject access/individuals rights;

12.5.9. to delete/return all Personal Data as requested at the end of the contract;

12.5.10. to submit to audits and provide information about the processing; and

12.5.11. to tell the Controller if any instruction is in breach of the GDPR or other EU or member state data protection law.

12.6. In addition the contract should set out:

12.6.1. The subject-matter and duration of the processing;

12.6.2. the nature and purpose of the processing;

12.6.3. the type of Personal Data and categories of individuals; and

12.6.4. the obligations and rights of the Controller.

13. INDIVIDUALS' RIGHTS

13.1. GDPR gives individuals more control about how their data is collected and stored and what is done with it. Some existing rights of individuals have been expanded upon and some new rights have been introduced. It is extremely important that Colleges plan how they will handle these requests under GDPR.

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

13.3. Subject Access Requests

13.3.1. Individuals have the right under the GDPR to ask a College to confirm what Personal Data they hold in relation to them and provide them with the data. This is not a new right but additional information has to be provided and the timescale for providing it has been reduced from 40 days to one month (with a possible extension if it is a complex request). In addition, you will no longer be able to charge a fee for complying with the request.

13.3.2. Subject Access Requests are becoming increasingly more common and 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.

13.4. Right of Erasure (Right to be Forgotten)

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

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

13.4.2. 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.

13.5. Right of Data Portability

13.5.1. 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:

13.5.1.1. the processing is based on consent or on a contract; and

13.5.1.2. the processing is carried out by automated means

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

13.6. The Right of Rectification and Restriction

13.6.1. 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.

13.7. 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.

14. MARKETING AND CONSENT

14.1. 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.

14.2. Marketing consists of any advertising or marketing communication that is directed to particular individuals. GDPR will bring about a number of important changes for organisations that market to individuals, including:

14.2.1. providing more detail in their privacy notices, including for example whether profiling takes place; and

14.2.2. rules on obtaining consent will be stricter and will require an individual's "clear affirmative action". The ICO like consent to be used in a marketing context.

14.3. Colleges also need to be aware of the Privacy and Electronic Communications Regulations (PECR) that sit alongside data protection. PECR apply to direct marketing i.e. a communication directed to particular individuals and covers any advertising/marketing material. It applies to electronic communication i.e. calls, emails, texts, faxes. PECR rules apply even if you are not processing any personal data.

14.4. Consent is central to electronic marketing. We would recommend that best practice is to provide an un-ticked opt-in box.

14.5. Alternatively, the College may be able to market using a “soft opt in” if the following conditions were met:

14.5.1. contact details have been obtained in the course of a sale (or negotiations for a sale);

14.5.2. the College are marketing its own similar services; and

14.5.3. the College gives the individual a simple opportunity to refuse to opt out of the marketing, both when first collecting the details and in every message after that.

15. AUTOMATED DECISION MAKING AND PROFILING

15.1. 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.

15.2. 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.

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

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

16. DATA PROTECTION IMPACT ASSESSMENTS (DPIA)

16.1. The GDPR introduce a new requirement to carry out a risk assessment in relation to the use of Personal Data for a new service, product or process. This must be done prior to the processing via a Data Protection Impact Assessment (“**DPIA**”). 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:

16.1.1. describe the collection and use of Personal Data;

16.1.2. assess its necessity and its proportionality in relation to the purposes;

16.1.3. assess the risks to the rights and freedoms of individuals; and

16.1.4. the measures to address the risks.

- 16.2. 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.
- 16.3. Where a DPIA reveals risks which are not appropriately mitigated the ICO must be consulted.
- 16.4. 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.
- 16.5. 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):
 - 16.5.1. 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;
 - 16.5.2. 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
 - 16.5.3. systematic monitoring of public areas on a large scale e.g. CCTV cameras.
- 16.6. All DPIAs must be reviewed and approved by the Data Protection Officer.

17. TRANSFERRING PERSONAL DATA

- 17.1. 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.
- 17.2. College Personnel must not export any Personal Data outside the EEA without the approval of the Data Protection Officer.

APPENDIX 1 – RELEVANT LEGISLATION

General Data Protection Regulation (GDPR) / Data Protection Act 2018 (DPA 2018)

GDPR and the DPA 2018 are the primary legislation covering personal information. They require that the processing of personal data complies with all of the principles specified under Article 5 of the GDPR, as follows:

- Processed lawfully, fairly and in a transparent manner.
- Collected for specified, explicit and legitimate purposes.
- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed.
- Accurate and, where necessary, kept up to date.
- Kept for no longer than is necessary for the purposes for which it is processed.
- Processed in a way that ensures it is appropriately secure.

The GDPR is retained in domestic law now the Brexit transition period has ended, but the UK has the independence to keep the framework under review. The 'UK GDPR' sits alongside an amended version of the DPA 2018.

For the purpose of this document, references to GDPR relate to the 'UK GDPR'.

Other legislation creates additional requirements relating to types and/or processing activities of personal data:

- Privacy and Communications (EC Directive) Regulations 2003 which apply to the use of personal data in direct marketing and other use of electronic communications.
- Computer Misuse Act 1990 which relates to unauthorised access or modification to computers.
- Freedom of Information Act 2000, which provides for access to all information held by public authorities.
- Protection of Freedoms Act 2012 which imposes specific requirements in relation to the biometric information.
- Regulation of Investigatory Powers Act (2000).
- Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000.

Legislation relating specifically to education also has implications for the processing of personal data.

General Data Protection Regulation (GDPR)

The GDPR (EU) 2016/679 is a regulation in EU law on data protection and privacy for all individuals within the European Union and the European Economic Area. It also addresses the export of personal data outside the EU and EEA. The GDPR aims primarily to give control to citizens and residents over their personal data and to simplify the regulatory environment for international business by unifying the regulation within the EU.

The GDPR details the statutory requirements for processing personal data. The Regulation includes the sanctions that apply in the event of a breach and misuse of personal information by individuals, including a criminal offence for disclosure of personal data which is unauthorised and carried out wilfully or negligently.

The GDPR is retained in domestic law now the Brexit transition period has ended, but the UK has the independence to keep the framework under review. The 'UK GDPR' sits alongside an amended version of the DPA 2018.

Data Protection Act 2018 (DPA 2018)

The Data Protection Act 2018 achieved Royal Assent on the 23rd May 2018. The 2018 Act modernises data protection laws in the UK to make the fit-for-purpose for our increasingly digital economy and society. The Act applies the EU's GDPR standards. Whereas the GDPR gives member states limited opportunities to make provisions for how it applies in their country, one element of the DPA 2018 is the details of these, applying as the national law.

Privacy & Electronic Communications (EC Directive) Regulations 2003

These regulations relate to direct marketing and make it unlawful to send someone direct marketing who has not previously given specific permission for their personal information to be used in this way (unless a previously existing relationship exists between the parties).

NB. There have been amendments to these regulations in 2004, 2011 and 2016.

Freedom of Information Act 2000 (FOI)

This statutory legislation places a requirement on all public bodies to manage records in such a way as to ensure that information is retained only as long as necessary and in such a way that it is identifiable and retrievable. The Act also allows any person to request any information held by a public authority. It is important to note that the Act applies only to certain parts the College and NES; more information is available in the FOI Policy.

Protection of Freedoms Act 2012

The Protection of Freedoms Act:

- places a requirement on Data Controllers in Schools and Colleges to obtain parental consent for the gathering of biometric data; and
- Regulates the use of CCTV for surveillance purposes.

Computer Misuse Act 1990

The purpose of this legislation is to secure computer material against unauthorised access or modification and for connected purposes; hacking and the introduction of viruses are criminal offences under this legislation.

Investigatory Powers Act 2016

This legislation limits and sets out circumstances in which individuals can be subjected to various forms of covert surveillance including telephone tapping, interception of correspondence and covert filming e.g. use of CCTV.

It specifically provides that the interception of private communications is unlawful other than where interception takes place in accordance with the provisions of the Act.

Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000

This legislation permits a business to intercept communications on its own network for business purposes and to detect email and internet abuse and to record telephone conversations to evidence transactions.

Education Specific Legislation and Statutory Guidance

There is a variety of legislation which creates either explicit or implied legal powers to collect, use and share personal data. (NB. this list is not exhaustive).

The Children Act (various dates) The Education Act (various dates) Education & Skills Act Various Department for Education Statutory Guidance.