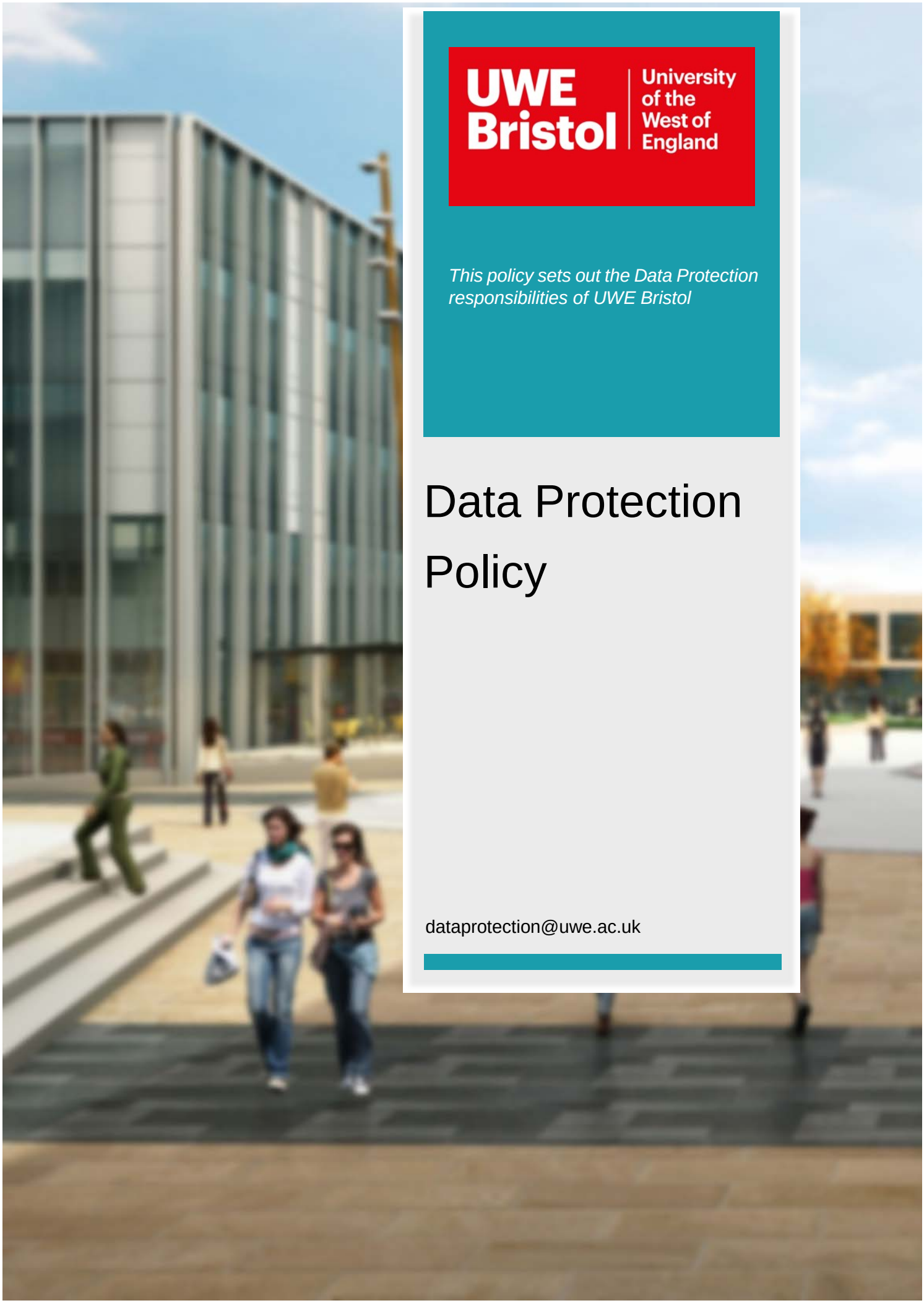

This policy sets out the Data Protection responsibilities of UWE Bristol

Data Protection Policy

dataprotection@uwe.ac.uk

Contents

1. Version Control

Written by (Contributors)	**James Whitbread (James Button & Jaz Clatworthy)**
Reviewed by	**Steven Dinning**
Approved by	**Directorate**
Published	**November 2019**
Next review (annual)	**November 2020**
Version	**1.0**

2. Purpose

The purpose of this policy is to:

- define the requirements of the General Data Protection Regulation (GDPR) as supplemented by The Data Protection Act 2018 (DPA 2018), in the context of the University of West of England (UWE Bristol);
- clarify responsibilities and duties and set out the structure within which they will be discharged

3. Scope

This policy applies to all personal information processed by, or on behalf of, UWE Bristol. This includes personal information accessed or used by UWE Bristol staff, as well as, for example, contractors, consultants and postgraduate research students engaged in UWE Bristol-led research.

The formats in which personal data is handled can range from electronic, hard copy, and voice recording formats, to spoken forms of communication. Definitions of data for the purposes of Data Protection can be found in Section 5 of this policy.

This policy also applies to de-identified (pseudonymised) personal data where individuals can be re-identified from other information e.g. student numbers and staff numbers.

4. Legislative Guidance

This policy is based on guidance published by the Information Commissioner's Office (ICO) on the GDPR and the ICO's code of practice for subject access requests.

It also reflects the ICO's code of practice for the use of surveillance cameras and personal information.

5. Definitions

Term	Definition
Personal data	Any information relating to an identified, or identifiable, individual. This may include the individual's: • Name (including initials) • Identification number • Location data • Online identifier, such as a username • It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.

Special categories of personal data	Personal data which is more sensitive and needs more protection, including information about an individual's: • Racial or ethnic origin • Political opinions • Religious or philosophical beliefs • Trade union membership • Genetics • Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes • Health – physical or mental • Sex life or sexual orientation
Processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.
Data subject	The identified or identifiable individual whose personal data is held or processed.
Data controller	A person or organisation that determines the purposes and the means of processing of personal data.
Data processor	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.
The University	University of West of England (UWE Bristol)

6. The data controller

The University processes personal data relating to students, parents, staff, governors, visitors and others, and therefore is a data controller.

UWE Bristol is registered as a data controller with the ICO (Z6686621) and will renew this registration annually or as otherwise legally required.

7. Roles and responsibilities

This policy applies to **all UWE Bristol staff** and **students**, and to external organisations or individuals working on the University's behalf. Individuals who do not comply with this policy may face disciplinary action.

7.1 Board of Governors

The Board of Governors have the overall corporate responsibility for ensuring that UWE Bristol complies with all relevant data protection legal obligations.

The University will ensure the Board of Governors receive sufficient information, in a timely manner, on the status of the University's data protection management system to satisfy themselves that all legal requirements are being met. They will be notified of any incidents carrying major risk to the safety and security of relevant personal data and any action taken by the regulatory authorities, and of any subsequent action taken by UWE Bristol.

7.2 Vice-Chancellor, President and Chief Executive Officer

UWE Bristol's Vice-Chancellor, President and Chief Executive Officer has overall responsibility for data protection management within the University and the implementation of its data protection policy. As the principal executive officer of the University, he acts as the representative of the data controller on a day-to-day basis.

7.3 Directorate

The Directorate provide senior level commitment to data protection management and provide oversight of the implementation and development of the University's data protection policy, associated policies and processes. The Directorate ensure co-ordination and consistency of data protection policies and processes across the University.

7.4 Assistant Vice-Chancellor: Data Protection & Dispute Management – UWE Bristol's Data Protection Officer

The Assistant Vice-Chancellor (AVC) provides strategic oversight of and direction for the management of the University's data protection & privacy obligations. The AVC discharges the role of UWE Bristol's nominated Data Protection Officer (DPO) and supervises the work of the Data Protection Office.

UWE Bristol's DPO is responsible for overseeing the implementation of this policy, monitoring the University's compliance with data protection law, and developing related policies and guidelines where applicable.

He will provide reporting of his activities directly to the Board of Governors and Directorate and, where relevant, report his advice and recommendations on UWE Bristol's data protection issues.

The DPO is also the first point of contact for individuals whose data UWE Bristol processes, and for the ICO.

Full details of the DPO's responsibilities are set out in his job description. UWE Bristol's DPO and UWE Bristol's Data Protection Office is contactable via dataprotection@uwe.ac.uk.

7.5 Chief Information Officer (CIO)

The CIO remains independent due to Director of Professional Service responsibilities but provides expert advice on data protection and information security matters and ensures appropriate information security and technical measures are in place and embedded within the University.

7.6 Head of Information Security

The Head of Information Security provides specialist information security services to the University including, information security incident response & remediation activities and information security consultancy for: strategic and infrastructure enabler projects, DPIAs, submissions, bids & tenders.

7.7 Pro Vice-Chancellors / Executive Deans of Faculty and Directors of Professional Services

Pro Vice-Chancellors / Executive Deans of Faculty and Directors of Professional Services demonstrate senior level commitment to data protection management and are accountable for the Faculty/Service's full range of data protection activities.

7.8 Heads of Department, Academic Leads and Line Managers

Heads of Department, Academic Leads and Line Managers ensure that the data protection policies & processes are made known, implemented and maintained within their areas of responsibility.

7.9 Data Protection Coordinators

Data Protection Coordinators (DPC) are a network of contacts in individual faculties and professional services that support the DPO in fulfilment of his duties. The DPC coordinates the data protection duties in a particular Faculty or Professional service.

7.10 All staff and postgraduate research students

Staff and postgraduate research students are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Informing UWE Bristol of any changes to their personal data, such as a change of address
- Contacting the DPO and/or their area DPC in the following circumstances:
    - With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
    - If they have any concerns that this policy is not being followed
    - If they are unsure whether or not they have a lawful basis to use personal data in a particular way

- If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the European Economic Area
- If there has been a data breach
- Whenever they are engaging in a new activity that may affect the privacy rights of individuals and may also require the completion of a Data Protection Impact Assessment (DPIA)
- If they need help with any contracts or sharing personal data with third parties

All staff are responsible for adhering to this policy as per the Terms & Conditions of employment.

7.11 All students

All students should:

- Co-operate with the University as far as is necessary to enable all data protection legal obligations and duties to be performed or complied with
- Report any suspected data protection incident to their tutor or to a responsible person within the university. This should be done by using the established reporting arrangement within their Faculty or Accommodation
- Undertake any data protection training and induction required by the University
- Receive appropriate supervision and support in safe and secure data protection management in relation to their research and related study activity

7.12 Data Protection Office

The Data Protection Office provides specialist advice and guidance to the Vice-Chancellor and the Directorate on relevant legislation and implementation of the University's Data Protection Policy. The Data Protection Office is also responsible for advising and supporting Executive Deans, Directors of Professional Services, Managers and all individuals on data protection issues at the University.

8. Data protection principles

The GDPR is based on data protection principles that UWE Bristol must comply with. The principles say that personal data must be:

- 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

This policy sets out how UWE Bristol aims to comply with these principles.

9. Collecting personal data

9.1 Lawfulness, fairness and transparency

UWE Bristol will only process personal data where the University has at least one of 6 'lawful bases' (legal reasons) to do so under data protection law:

- The data needs to be processed so that the University can **fulfil a contract** with the individual, or the individual has asked UWE Bristol to take specific steps before entering into a contract
- The data needs to be processed so that UWE Bristol can **comply with a legal obligation**
- The data needs to be processed to ensure the **vital interests** of the individual e.g. to protect someone's life
- The data needs to be processed so that UWE Bristol, as a public authority, can perform a task **in the public interest,** and carry out its official functions
- The data needs to be processed for the **legitimate interests** of the University or a third party (provided the individual's rights and freedoms are not overridden)
- The individual (or their parent/carer when appropriate in the case of a student) has freely given clear **consent**

For special categories of personal data, UWE Bristol will also, in addition to one of the 6 lawful bases, meet one of the special category conditions for processing which are set out in the GDPR Article 9 and Data Protection Act 2018. When processing special category and criminal convictions data, in addition to this policy, the University will also adhere to its Data Protection: Processing Special Category Data and Criminal Convictions Data Policy.

Whenever UWE Bristol first collects personal data directly from individuals, UWE Bristol will provide them with the relevant information required by data protection law on how their data is processed through the use of the relevant privacy notice.

9.2 Limitation, data minimisation and accuracy

UWE Bristol will only collect personal data for specified, explicit and legitimate reasons. The University will explain these reasons to the individuals when UWE Bristol first collect their data by issuing them with the relevant privacy notice.

If the University wants to use personal data for reasons other than those given when originally obtained, UWE Bristol will inform the individuals concerned before proceeding, and seek consent where necessary.

Staff must only process personal data where it is necessary in order to fulfil their job role.

When staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done as set out in UWE Bristol's privacy notices available on UWE Bristol's website.

10. Sharing personal data

UWE Bristol will not normally share personal data with anyone else, but may do so where:

- There is an issue with a student or parent/carer that puts the safety of our staff at risk
- UWE Bristol needs to liaise with other agencies – the University will seek consent if any other lawful bases cannot be relied upon before doing this
- The University's suppliers or contractors need data to enable us to provide services to staff and students. When doing this, UWE Bristol will:
    - Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law
    - Establish a Data Processing Agreement with the supplier or contractor, if they're a Data Processor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data UWE Bristol share
    - Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us

UWE Bristol will also share personal data with law enforcement and government bodies where the University is legally entitled to do so, including for:

- The prevention or detection of crime and/or fraud
- The apprehension or prosecution of offenders
- The assessment or collection of tax owed to HMRC
- In connection with legal proceedings
- Where the disclosure is required to satisfy UWE Bristol's safeguarding obligations
- Research and statistical purposes, providing Article 89 safeguards have been met, for example that personal data is sufficiently anonymised or consent has been provided

UWE Bristol may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of our students or staff.

Where UWE Bristol transfers personal data to a country or territory outside the European Economic Area, the University will do so in accordance with data protection law.

11. Subject access requests and other rights of individuals

11.1 Data subject rights

Please refer to UWE Bristol's Statement of Intent: Data Subject Rights for further detailed information on the recognised rights of, and guidance for, Data Subjects.

11.2 Subject access requests

Individuals have a right to make a 'subject access request' to gain access to personal information that UWE Bristol holds about them. This includes:

- Confirmation that their personal data is being processed
- Access to a copy of the data
- The purposes of the data processing

- The categories of personal data concerned
- Who the data has been, or will be, shared with
- How long the data will be stored for, or if this isn't possible, the criteria used to determine this period
- The source of the data, if not the individual
- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual

Subject access requests should be submitted in writing, either by letter, email or fax to the Data protection office. They should include:

- Name of individual
- Correspondence address
- Contact number and email address
- Details of the information requested

If any staff receive a subject access request they must immediately forward it to the Data Protection Office.

11.3 Children and subject access requests

Personal data about a child belongs to that child, and not the child's parents or carers. For a parent or carer to make a subject access request with respect to their child, the child must either be unable to understand their rights and the implications of a subject access request, or have given their consent.

Children aged 12 and above are generally regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of children at, or who interact with UWE Bristol, may not be granted without the express consent of the child. This is not a rule and a child's ability to understand their rights will always be judged on a case-by-case basis.

11.4 Responding to subject access requests

When responding to requests, UWE Bristol:

- May ask the individual to provide 2 forms of identification
- May contact the individual via phone to confirm the request was made
- Will ordinarily respond without delay and within 1 month of receipt of the request
- Will provide the information free of charge
- May tell the individual that UWE Bristol will comply within 3 months of receipt of the request, where a request is complex or numerous. The University will inform the individual of this within 1 month, and explain why the extension is necessary

UWE Bristol will not disclose information, for example if it:

- Might cause serious harm to the physical or mental health of the subject or another individual

- Would reveal that the subject is at risk of abuse, where the disclosure of that information would not be in the subject's best interests
- Is given to a court in proceedings concerning the subject
- Results in the disclosure of information relating to another individual who can be identified and where such information cannot be reasonably or sufficiently redacted by the University

UWE Bristol may redact information from a subject access request disclosure. For example, if it:

- Enables the University to fulfil the subject access request without breaching the data protection principles
- Is out of scope of the subject access request because it is not the applicant's personal data

If the request is unfounded or excessive, UWE Bristol may refuse to act on it, or charge a reasonable fee which considers administrative costs.

A request will be deemed to be unfounded or excessive if it is repetitive, or asks for further copies of the same information.

When UWE Bristol refuse a request, the University will tell the individual why, and tell them they have the right to complain to the ICO.

11.5 Other data protection rights of the individual

In addition to the right to make a subject access request, and to receive information when UWE Bristol are collecting their data about how UWE Bristol use and process it (see section 9), individuals also have the right to:

- Withdraw their consent to the processing of data, where consent is needed to process it, at any time
- Ask the University to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Challenge processing which has been justified on the basis of public task and legitimate interest
- Request a copy of agreements under which their personal data is transferred outside of the European Economic Area
- Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them)
- Prevent processing that is likely to cause damage or distress
- Be notified of a data breach in certain circumstances
- Make a complaint to the ICO
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)

Individuals should submit any request to exercise these rights to the Data Protection Office. If staff receive such a request, they must immediately forward it to the Data Protection Office.

The above rights apply only in certain circumstances. They are not absolute or unqualified rights. Guidance can be provided by the Data Protection Office in each individual case.

12. CCTV and ANPR

The University uses CCTV and ANPR in various locations around all UWE Bristol sites to ensure it remains safe. UWE Bristol will adhere to the ICO's code of practice for the use of CCTV.

UWE Bristol do not need to ask individuals' permission to use CCTV and ANPR, but UWE Bristol make it clear where individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining their use.

Any enquiries about the CCTV system and ANPR should be directed to the Data Protection Office.

13. Photographs and videos

As part of UWE Bristol activities, UWE Bristol may take photographs and record images of individuals within UWE Bristol.

UWE Bristol will obtain written consent from students aged 18 and over, for photographs and videos to be taken of students for communication, marketing and promotional materials.

Whether the University requires your consent or not, UWE Bristol will clearly explain to the subject how the photograph and/or video will be used.

Uses may include:

- Within UWE Bristol on notice boards and in UWE Bristol magazines, brochures & newsletters
- Outside of the University by external agencies such as an UWE Bristol photographer, newspapers and/or campaigns
- Online on UWE Bristol's website or social media pages

Consent can be refused or withdrawn at any time. If consent is withdrawn, UWE Bristol will delete the photograph or video and not distribute it further.

When using photographs and videos in this way UWE Bristol will not accompany them with any other personal information about the student, to ensure they cannot be identified.

For more information on our use of photographs and videos please contact the Data Protection Office.

14. Data protection by design and default

The University will put measures in place to show that UWE Bristol have integrated data protection into all data processing activities, including:

- Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge
- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law (see section 8)

- Completing Data Protection Impact Assessments (DPIAs) where UWE Bristol's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the Data Protection Office and DPO will advise on this process)
- Integrating data protection into internal documents including this policy, any related policies and privacy notices
- Regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters; UWE Bristol will also keep a record of completion and/or attendance
- Regularly conducting reviews and audits to test privacy measures and make sure UWE Bristol are compliant with GDPR
- Maintaining records of our processing activities, including:
    - For the benefit of data subjects, making available the contact details of the University's DPO and all information UWE Bristol is required to share about how personal data is processed (via privacy notices)
    - For all personal data that UWE Bristol holds, maintaining an internal record of the type of data, data subject, how and why UWE Bristol are using the data, any third-party recipients, how and why the University are storing the data, retention periods and how UWE Bristol are keeping the data secure

It is the responsibility of all staff and post-graduate research students to incorporate data protection by design and default into all activities, processes or projects that may involve the use of personal data. This includes undertaking a Data Protection Impact Assessment (DPIA) to establish the controls needed for protecting personal data. Methods of control include, for example, encryption, anonymisation and pseudonymisation. Guidance on conducting Data Protection (Privacy) Impact Assessments is available on the intranet (UWE Bristol Staff link only).

15. Data security and storage of records

UWE Bristol will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage.

In particular:

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data are kept under lock and key when not in use
- Papers containing confidential personal data must not be left on office and classroom/lecture theatre desks, on staffroom tables, pinned to notice/display boards, or left anywhere else where there is general access
- Where personal information needs to be taken off site, staff must ensure normal workplace data protection measures are observed
- Passwords adhere to UWE Bristol policy and published guidance which can be found on UWE Bristol's website
- Where USB devices are identified as a need for use, the Data Protection Protocols (UWE Bristol Staff link only) guidance is adhered to
- Where exceptionally and in accordance with approved UWE Bristol policy, staff, students or governors are storing or using personal information on their personal

devices, are expected to follow the same security procedures as for UWE Bristol-issued equipment

- Where the University needs to share personal data with a third party, UWE Bristol carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected (see section 10)

16. Disposal of records

Personal data that is no longer needed by the University will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where UWE Bristol cannot or do not need to rectify or update it.

For example, UWE Bristol will shred or incinerate paper-based records, and overwrite or delete electronic files and backups. The University may also use a third party to safely dispose of records on UWE Bristol's behalf. UWE Bristol will require the third party to provide sufficient guarantees that it complies with data protection law.

Please refer to UWE Bristol's Records Management Policy for further detailed information on the appropriate creation, maintenance, storage, use and disposal of UWE Bristol records and retention schedules.

17. Personal data breaches

UWE Bristol will make all reasonable endeavours to ensure that there are no personal data breaches.

17.1 Data breach procedure

In the unlikely event of a suspected data breach, UWE Bristol will follow the procedure set out in the University's Data Breach Management Plan (UWE Bristol staff link only) which is based on guidance on personal data breaches produced by the ICO.

17.2 Data breach reporting guidance for staff

All UWE Bristol staff should follow the Data Breach Reporting guidance (UWE Bristol Staff link only) if they suspect a potential data breach has occurred.

If it is determined by the University that a data breach has occurred, depending upon the seriousness and complexity of the incident, an Incident Response Team may be set up, comprising appropriate University expertise to ensure that the incident is managed appropriately. Following the immediate containment of the breach, the risks associated with the breach will be assessed in order to identify an appropriate response. All data security breaches must be managed according to the severity of the risk they pose.

When appropriate, UWE Bristol will report the data breach to the ICO within 72 hours.

18. Training

All staff and governors are required to complete data protection training as part of their mandatory induction process.

Data protection will also form part of continuing professional development, where changes to legislation, guidance or UWE Bristol's processes make it necessary.

19. Policy monitoring

The DPO is responsible for monitoring and reviewing this policy.

This policy shall be reviewed annually, or more frequently if appropriate, to reflect relevant legislative, regulatory, or organisational developments.

20. Related Policies

This data protection policy is linked to our:

- Information Security Policy
- Information Handling Policy
- Acceptable Use Policy
- Remote Access Policy

21. Related procedures

- Information Security Toolkit
- Data Breach Reporting Guidance
- Data Breach Management Procedure (for use by UWE Bristol DPO and Data Protection Coordinators
- UWE Bristol Internal Data Protection Guide / Manual (for use by UWE Bristol Data Protection Office and Data Protection Coordinators)