



UCFB* Data Protection Policy

Owner:	Director of Transformation, Technology, Facilities and Sport
Author:	Head of Transformation & Technology
Version Number:	1.1
Approval Date:	8 July 2026
Approved By:	Board of Directors
Date of Commencement:	01 September 2026
Date of Last Review:	June 2026
Date for Next Review:	June 2027

*UCFB is trading name of University Campus of Football Business Limited

1. Summary

- This Policy applies to any data that could identify an individual either directly or in combination with other data that you may hold or come into possession of this is known as **personal data**.
- Some types of personal data are particularly sensitive. This is referred to as **special category data**, which must be treated particularly carefully. Special category data includes information such as data about race, ethnicity, religion, medical/health data, political affiliations, genetic or biometric information. Further information on how and why we process special category data can be found in **Appendix 1: Sensitive Data Category**.
- Complying with this Policy is a condition of employment or study at UCFB. Non-compliance with the obligations within this Policy may result in disciplinary action.
- Misuse of data or negligent disregard for the obligations contained within the Data Protection Act 2018 (DPA), or any law designed to protect personal data, could lead to prosecution and a criminal record.
- This Policy explains how UCFB meets its obligations under the DPA and outlines the responsibilities of staff and students when they collect, use, or process personal data.
- This Policy forms part of UCFB's information governance framework (see Section 22 (below)), which is based on: the requirements of a BS10012:2017, which is a quality standard that sets requirements on how we collect, store, use, share and dispose of personal data as well as how we react in the event of a personal data breach; ongoing compliance with data protection and other information laws; Office for Students requirements; and the implementation of information governance best practices across the institution.
- UCFB must provide information about any processing of personal data taking place and ensure that individuals are aware of and can exercise their information rights.
- All staff, students and third parties associated with UCFB have a responsibility to ensure that they keep personal data secure, only share it when authorised, and only use personal data for the purpose it was collected. Any students that process the personal data of others as part of their course are subject the same conditions and to the relevant points in this Policy.
- Personal data processed for UCFB purposes on personal devices is still subject to the obligations of data protection legislation, Office for Students requirements, and other applicable professional, statutory, or regulatory bodies. If you have a non-UCFB managed device, and process personal data (for example in an instant messaging application) you must comply with the data protection principles.
- In the event of a data breach or a suspected breach, staff and students have a responsibility to notify the Data Protection Officer via: dataprivacyteam@UCFB.ac.uk as soon as possible.
- The UCFB Data Protection Team provides a range of resources and guidance to help Academic Centres and departments comply with information law.
- A glossary of commonly used terminology and definitions is provided in **Appendix 2: Glossary**.

2. Scope

This Policy applies to any individual or organisation that processes personal data for, or on behalf of, UCFB or another business affiliated with our activities. Processing of personal data occurs when an action is carried out on the personal data to complete a function. Processing activities include, but are not limited to, the identification, collection, recording, organising, structuring, storage, alteration, retrieval, consultation, use, disclosure by any means, restriction, erasure or destruction of personal data.

This Policy applies to all processing of personal data in electronic form including electronic mail, documents created with word processing software, applications, software or where it is held in manual files that are structured in a way that allows ready access to information about individuals. This Policy establishes a minimum standard for the processing and protection of personal and sensitive category data by all UCFB entities. If there are any conflicts between this Policy and national law, the law will take precedence. In this case, please consult with the Data Privacy Team for guidance.

3. Purpose of Data Collection and Processing

UCFB needs to collect and store a wide range of personal (see also **Appendix 3: Examples of Personal Data** (below)) and special category data about its employees, students and other users of UCFB facilities to allow it to maintain its core operations. To comply with the law, UCFB and anybody responsible for processing personal data on its behalf must:

- Be accountable and transparent about how and why we use personal data;
- Implement the appropriate controls, technical and organisational measures required to demonstrate compliance with the data protection principles;
- Allow a person to exercise their Information Rights and adhere to approved codes of conduct for data protection;
- Only use personal data for clear and specified purposes;
- Only keep personal data for as long as is reasonably required;
- Ensure that personal data is kept securely and protected against unlawful processing, accidental or deliberate loss, destruction or damage.

4. Data Protection Principles

The following principles govern the collection, use, retention, transfer, disclosure and destruction of personal data. These principles must be followed when processing personal data. Further advice and guidance about how to apply these principles can be obtained from the Data Privacy Team.

- **Lawfulness, Fairness and Transparency** - Personal data shall be processed lawfully, fairly and in a transparent manner;
- **Purpose Limitation** - Personal data shall be collected for specified, explicit and legitimate purposes and not used for other purposes where such use would be incompatible with the initial purpose;
- **Data Minimisation** - Personal data shall be adequate, relevant and limited to what is necessary for the purpose it was collected;
- **Accuracy** - Personal Data shall be accurate and, where necessary kept up to date.
- **Storage Limitation** - Personal data shall be kept in a form, which permits identification of Data Subjects for no longer than is necessary;
- **Integrity & Confidentiality** - Personal data shall be processed in a manner that ensures appropriate security including protection against unauthorised or unlawful processing, and against accidental loss, destruction or damage to that data; and
- **Accountability** - UCFB must be able to demonstrate how we comply with the law by ensuring that we have documented processes, procedures and policies in place.

Responsibilities: The Board of Directors has delegated the responsibility for the protection of personal data at Senior Management Team level to a dedicated Data Protection Officer (DPO). The DPO is authorised to act independently and has overall responsibility for ensuring ongoing compliance with UCFB's data protection obligations. In order to comply with obligations, set out in the UK General Data Protection Regulation, Data (Use and Access) Act 2025 (DUAA), and other applicable regulations, the role of the DPO is autonomous and they report to the highest level of management within the organisation. The DPO is also the first point of contact for supervisory authorities and for individuals whose data is processed. Each Dean, Deputy Dean and/or Director/Head of Service is responsible for promoting and modelling best practice regarding data protection within their teams and keeping the DPO informed of changes in the collection, use, and security measures used for the processing of personal data within the Academic Centre, Service or Team. To meet this requirement, the Data Privacy Team will train UCFB staff to act as data protection advisors responsible for promoting best practices and reporting issues within their own departments. Senior Management, staff, and students all have responsibilities in relation to data protection, which are highlighted in **Appendix 4: Responsibilities** (below).

Where processing of personal or special category data will involve new technology or high-risk activities such as a high degree of monitoring or profiling, a Data Privacy Impact Assessment may need to be conducted. A Data Protection Impact Assessment template will be established and maintained by the Data Privacy Team, with will also provide associated advice and guidance. Business Owners are responsible for ensuring that any risks identified in a Data Protection Impact Assessment are mitigated to a level that falls within the institutional risk appetite.

5. Information Rights

Every person about whom UCFB processes personal data has rights associated with how the data is used and managed. Where an individual makes a request related to any of their information rights, UCFB will consider each request in accordance with all applicable laws and regulations. Every user that processes personal data for UCFB purposes is required to co-operate with the Data Privacy Team in complying with our obligations around responding to information rights requests. A breakdown of these rights and the process for putting in a request relating to information rights, is listed in **Appendix 5: Information Rights** (below).

6. Fair Processing Notices

Where UCFB acts as a Data Controller, we will provide information about how it processes the personal data of data subjects and our purposes for processing that data. We will also identify the circumstances under which transfers take place and provide information about routine disclosures to other parties and recipients. A complete list of UCFB's Fair Processing Notices is listed in **Appendix 6: Fair Processing Notices** (below).

7. Information Security

All staff and students are responsible for ensuring that:

- Any personal data which they hold in whatever format is kept securely;
- Personal data is not disclosed either orally, in writing or electronically either accidentally or otherwise to any unauthorised third party;
- Personal data that is taken off site is not left unattended or unsecured;
- Desks are kept clear of personal data when unattended;
- Where personal information exists in a manual form, it should be kept in a locked filing cabinet, drawer or in a secured area.

Where personal data is held in an electronic form, each Dean of Academic Centre or Director/Head of Service is responsible for ensuring that appropriate technical and organisational measures are taken to ensure against unauthorised or unlawful processing of personal data and against accidental loss/ destruction of/damage to such data. This includes data that is held by a third party such as a cloud services provider. Examples of such measures include:

- Encryption of personal data in transit and at rest;
- Secure retention or disposal of personal data in a timely fashion;
- Limiting access as necessary and proportionate for the purpose;
- Ensuring that the system meets the technical requirements needed to fulfil any type of Information Rights request;
- Where held internally the data is held on UCFB SharePoint, or within the UCFB Office 365 environment;
- Where held by a Data Processor or third party, the data is located within the European Union; and
- Limiting the sharing of data to what is proportionate and necessary to achieve the purposes.

8. Use of UCFB Email

The use of the UCFB email system should be used to communicate UCFB business in line with our email policies. The use of personal email addresses for UCFB business for

staff and students is not permitted where access to UCFB email systems is available. While the use of email attachments is permitted for general business, documents containing personal or special category data should be shared using SharePoint, OneDrive for Business or Microsoft Teams. When sending personal data externally, SharePoint should be used where available. As an alternative, documents can be password protected and sent as an email attachment.

9. Remote Working

When working remotely, the principles and obligations of the Data Protection Act 2018 (DPA) still apply. All staff are expected to ensure that any data they process from home (including on their own personal devices or in paper form) is kept secure and separate from other files or documents. The data in certain applications such as Office 365 will be protected using multi-factor authentication and other measures including the encryption of data and the potential restriction of downloading and sharing functionalities. When using personal equipment such as laptops, staff are expected to ensure that software is kept up to date and anti-virus software is installed. Where you need to share data, staff must use their UCFB email, Microsoft Teams, OneDrive or SharePoint accounts. The sharing of UCFB data using personal email addresses or personal cloud storage or communications platforms is not permitted.

10. Recommended Software and Systems

IT Services offer and support a range of systems, applications and services to meet UCFB's core business purposes. These supported systems have been assessed to ensure that they meet our requirements on functionality, storage of data, disaster recovery, security and regulatory compliance with data protection and other relevant laws. Any staff or students that wish to use applications, software or services that are not recommended by IT Services are responsible for ensuring that appropriate controls are in place to allow UCFB to comply with the obligations of the DPA and other relevant laws. Due to the complex nature of compliance, it is strongly recommended that you check with IT Services before using new systems, apps, or services. The Data Privacy Team will assist in assessing compliance, where appropriate however, you must notify the Data Privacy Team or delegated representative that an assessment of an unsupported application, system or service is required **before** personal data is processed.

Where use of an unsupported system, application or service is deemed to create a risk to UCFB, the Data Protection Officer or delegated representative will present these risks, along with proposed steps to mitigate them. If you choose not to implement the suggested mitigations and accept the level of risk, the Data Privacy Team will seek acceptance of these risks using a risk assessment form signed by the appropriate Dean, Deputy Dean or Director/Head of Service, which will be kept under regular review.

In cases where there is potential of such systems, applications or services to breach our obligations around data protection (e.g. not comply with the data protection principles) the Data Protection Officer has a legal obligation to highlight this potential breach to the relevant Dean, Deputy Dean or Director/Head of Service and, if necessary, the Executive Leadership Team and/or the Information Commissioners Office. Such breaches place a legal obligation on UCFB to stop processing the

personal data in a way that breaks the law and, in such cases, immediate steps will be taken by the Data Privacy Team to ensure UCFB remains compliant with its obligations.

11. Publication of UCFB Information

As a public authority subject to the Freedom of Information Act 2000, it is the policy of UCFB to make public as much information about the institution as possible. In particular, the following personal data will be available to the public for inspection via our website, annual accounts, or by submission of a Freedom of Information Request:

- Names of Officers of UCFB;
- Names of our Board of Directors;
- Names and job titles of the Executive Leadership Team;
- Names and job titles of members of the Senior Leadership Team;
- Staff lists and areas of expertise; and
- Names and job titles of senior staff.

If an individual wishes any details, in the categories listed above, to be confidential and has good reason for this, they must contact the DPO who will consult with the Director of Student and Academic Services. The disclosure of personal data to third parties under the Freedom of Information Act will be reviewed on a case-by-case basis and must always comply with the data protection principles described above.

12. Law Enforcement Requests & Disclosures

In certain circumstances, personal data will be shared without the knowledge or consent of a Data Subject. This is the case where the disclosure of the personal data is necessary for any of the following purposes:

- The prevention or detection of crime;
- The apprehension or prosecution of offenders;
- The assessment or collection of a tax or duty; and/or
- By the order of a court or by any rule of law.

If UCFB or a known third-party processes personal data for one of these purposes, then it may apply an exception to the processing rules outlined in this Policy but only to the extent that not doing so would be likely to prejudice a potential investigation. If any UCFB employee receives a request from a court or any regulatory or law enforcement authority for information relating to personal data held by UCFB, the request must be directed to the Data Protection Officer, who will provide comprehensive guidance and assistance.

13. Data Protection Training

All UCFB employees, contractors, temporary staff and volunteers that have access to personal data will have their responsibilities under this Policy outlined to them as part of their staff induction training, which will include data protection training. For areas that process high volumes of personal data or special category data, bespoke data protection training is available. The Data Privacy Team will ensure that all UCFB staff and students have access to information that outlines key responsibilities and contains resources for ensuring that that UCFB can demonstrate compliance.

14. Data Sharing and Transfers

UCFB may share or transfer personal data or special category data to internal recipients or other organisations to provide services on our behalf (Data Processors). In some cases, such transfers may take place outside of the EU. UCFB and its entities will only transfer or share personal data to, or allow access by, third parties when it is assured that the information will be processed legitimately and protected appropriately by the recipient and/or data processor. Processes for data sharing and transfers can be found in **Appendix 7: Data Sharing and Transfers** (below).

15. Complaints Handling

Data Subjects with a complaint about the processing of their personal data should put forward the matter in writing to the Data Privacy Team via: DataPrivacyTeam@ucfb.ac.uk in the first instance. Complaints will be considered on a case-by-case basis, and where applicable an investigation will be conducted. The DPO or a nominated representative will inform the Data Subject of the progress and the outcome of the complaint within a reasonable period. If the issue cannot be resolved through consultation between the Data Subject and DPO, or appointed representative, then the Data Subject may, at their own cost, seek redress through mediation, binding arbitration, litigation, or via complaint to the supervisory authority within the applicable jurisdiction. In the United Kingdom, the Information Commissioners Office acts as an independent regulator for this purpose.

16. Breach Reporting

Any individual who suspects that a personal data breach has occurred due to the theft, loss, or exposure of personal data must immediately notify the DPO providing a description of what occurred. Notification of the incident can be made via e-mail at: DataPrivacyTeam@ucfb.ac.uk. The DPO or an appointed representative will investigate all reported incidents to confirm if a personal data breach has occurred. If confirmed, the DPO will follow the relevant authorised procedure based on the criticality and quantity of the personal data involved. For severe personal data breaches, the DPO will initiate and chair an emergency response team to coordinate and manage the personal data breach response, including notifying the relevant supervisory authority if appropriate.

17. Research Purposes Exemption

The Data Protection Act 2018 (DPA) contains specific exemptions for the use of personal data in scientific, statistical or historical research. Personal data collected fairly and lawfully for the purpose of one piece of research can be used for other research, providing that the final results of the research do not identify the individual. Such data must not be processed in such a way that leads to direct consequences for the individual concerned, or in a way that is likely to cause substantial damage or distress to any Data Subject. Records or questionnaires may be kept in order that the data can be revisited and re-analysed. This exemption is only applicable to academic research and cannot be used for commercial, or market research purposes. For further information on data protection in research please email DataPrivacyTeam@ucfb.ac.uk.

18. Retention of Data

UCFB will keep some forms of information for longer than others, in accordance with legal, financial, archival, or other business requirements. In accordance with the storage limitation principle, UCFB will dispose of any personal data for which it no longer has a specified purpose. In order to apply consistent retention periods to our most commonly collected data, we have produced a Records Lifecycle Management Scheme that sets out current retention periods.

19. CCTV

UCFB has in place CCTV surveillance systems across its UK campuses. UCFB has its own CCTV systems in place and identified properties (such as Arch View House, Quay Plaza, Piccadilly Place Study Hub) and Landlord's also have their own CCTV systems operational (Wembley Stadium, Old Trafford Football Stadium, etc.). The [UCFB Group CCTV Policy](#) details the purpose, use and management of the CCTV systems at UCFB and defines the procedures to be followed in order to ensure that UCFB complies with relevant legislation and the current Information Commissioner's Office Code of Practice. UCFB will have due regard to the UK General Data Protection Regulation ("UK GDPR"), the Data Protection Act 2018 ("DPA 2018"), the Data (Use and Access) Act 2025 (DUAA), and any subsequent data protection legislation, the Protection of Freedoms Act 2012 and the Human Rights Act 1998. Although not a relevant authority, UCFB will also have due regard to the Surveillance Camera Code of Practice, issued under the Protection of Freedoms Act 2012 and in particular the 12 guiding principles contained therein.

20. Monitoring of networks and accounts

UCFB takes a range of proactive measures to protect personal data, its technology, infrastructure, computer networks and intellectual property. Every user of our network is issued with a unique username and password to their own user account. Any actions taken on this account are logged and can be audited by IT Services. This includes but is not limited to:

- Any websites visited while logged in to your UCFB account;
- Any email that is sent or received by your UCFB email address; and
- Any instant messages sent or received by Microsoft Teams.

UCFB utilises Data Loss Prevention technology to reduce the risk of high volumes of personal data leaving our network via any Office 365 pathway including by email, OneDrive for Business or SharePoint. Where we get an alert that such activity has taken place, our Data Privacy Team will investigate to ensure that the disclosure of personal data remains compliant with information law.

21. Data Protection Offences

Under the Data Protection Act 2018 (DPA), it is an offence to:

- Obtain, disclose, sell or offer to sell personal data from UCFB systems without the consent of UCFB;
- Retain personal data outside the scope of your role or following the end of your employment without the consent of UCFB;
- Alter, destroy or conceal personal data to prevent a legitimate disclosure; and/or
- Recklessly re-identify personal data that has been de-identified without the consent of UCFB.

If there is evidence of an offence under the DPA, the matter will be subject to an investigation under our disciplinary procedures. Where it is found that an offence has been committed, sanctions may include dismissal or expulsion. In some circumstances, we have a legal duty to report offences to Information Commissioners Office.

22. Related Policies and Procedures

- [UCFB Group CCTV Policy](#)
- [UCFB Data Privacy Notice](#)
- [UCFB Records Management Policy](#)
- [UCFB Records Lifecycle Management Scheme](#)
- [UCFB Information Security Policy](#)

Appendix 1: Sensitive Data Category

Understanding the Sensitive Data Category

The Data Protection Act 2018 (DPA) is based around seven principles of 'good information handling'. These principles give people specific rights in relation to their personal information and place certain obligations on those organisations that are responsible for processing it. If we hold information about individuals either on computer, in a manual form such as paper or in certain types of filing system, we may be holding 'personal data.' How and why we hold and use this personal data determines if UCFB is following the DPA. Some personal data is particularly sensitive. In such cases, it is called 'Sensitive Category' data. Sensitive Category data needs more protection and examples would include information about a person's

- race;
- ethnic origin;
- politics;
- religion;
- trade union membership;
- genetics;
- biometrics (where used for ID purposes);
- health;
- sex life; and/or
- sexual orientation.

This type of data needs additional protection because if it was lost, disclosed in error, or destroyed by accident could create more significant risks to a person's fundamental rights and freedoms. For example, by putting them at risk of unlawful discrimination. Personal data relating to criminal convictions and offences are not included, but similar extra safeguards apply to its processing.

Handling Special Category Data

Because of the increased risks associated with handling Special category data, it is important that it be handled with care and consideration. Key things to bear on mind are:

- Sensitive Category Data must only be used if UCFB can demonstrate it has a legal reason to use and process it;
- It must be limited to the minimum necessary for us to do what we need to do with it;
- It must be kept secure;
- It must only be shared when necessary; and
- It should only be collected when someone understands why it is necessary.

Keeping Special Category Data Secure

Using good security practices can significantly reduce the risk of something going wrong such as losing data or disclosing it in error. Simple measures vastly reduce the risks:

- Lock away paper with lots of personal data when you are away from your desk or its unattended;
- If your sharing a file internally send it via OneDrive for Business or SharePoint rather than email attachment;
- If sharing externally make sure to double check the recipient of the data and consider password protecting the file;
- If you have used data for its purpose and don't need the raw data anymore, get rid of it; and
- Don't keep unnecessary duplicates.

Appendix 2: Glossary

Anonymisation: Data amended in such a way that no individuals can be identified from the data (whether directly or indirectly) by any means or by any person.

Consent: Any freely given, specific, informed and unambiguous indication of the Data Subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the Processing of Personal Data relating to him or her.

Data controller: A natural or legal person, Public Authority, Agency or other body which, alone or jointly with others, determines the purposes and means of the Processing of personal data.

Data processor: A natural or legal person, Public Authority, Agency or other body which Processes Personal Data on behalf of a Data Controller.

Data protection: The process of safeguarding Personal Data from unauthorised or unlawful disclosure, access, alteration, Processing, transfer or destruction.

Data Protection Officer (DPO): The DPO is responsible for informing and advising the organisation and its employees about their obligations to comply with the UK GDPR and other data protection laws.

Data Subject: The identified or Identifiable Natural Person to which the data refers.

Encryption: The process of converting information or data into code, to prevent unauthorised access.

Employee: An individual who works part-time or full-time for UCFB under a contract of employment, whether oral or written, express or implied, and has recognised rights and duties. Includes temporary employees and independent contractors.

Identifiable Natural Person: Anyone who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Personal data: Any information (including opinions and intentions) which relates to an identified or Identifiable Natural Person or Data Subject.

Personal data breach: A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed unknowingly or without authorisation

Process, Processed, Processing: Any operation or set of operations performed on personal data or on sets of personal data, whether or not by automated means. Operations performed may include:

- Collection;
- Recording;
- Organisation;
- Structuring;
- Storage;
- Adaptation;
- Alteration;

- Retrieval;
- Consultation;
- Use;
- Disclosure by transmission, dissemination or otherwise making available;
- Alignment or combination;
- Restriction;
- Erasure; and
- Destruction.

Profiling: Any form of automated processing of Personal Data where personal data is used to evaluate specific or general characteristics relating to an Identifiable Natural Person. Particularly to analyse or predict certain aspects concerning that natural person's performance at work, economic situations, health, personal preferences, interests, reliability, behaviour, location or movement.

Pseudonymisation Data amended in such a way that no individuals can be identified from the data (whether directly or indirectly) without a "key" that allows the data to be re-identified.

Special Categories of Data: Personal data pertaining to or revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership; data concerning health or sex life and sexual orientation; genetic data or biometric data.

Supervisory authority: An independent Public Authority responsible for monitoring the application of the relevant data protection regulation set forth in national law. In the UK the Information Commissioners Office acts as a supervisory authority.

Third Country: Any country not recognised as having an adequate level of legal protection for the rights and freedoms of Data Subjects in relation to the processing of personal data.

1. **Third Party:** An external organisation with which UCFB conducts business and is also authorised to, under the direct authority of UCFB, process the personal data under the responsibility of UCFB as a data controller.

UEL Entity: A UCFB establishment, including subsidiaries and joint ventures over which UCFB exercise management control.

Appendix 3: Examples of personal data

Personal data includes:

- Staff and student records;
- Alumni data;
- Applicant data;
- Examination marks;
- Research data;
- Electronic data relating to personal devices, images and audio records;
- Residence and catering information;
- Details of financial transactions; and
- Other information about its staff, students and affiliates which enables UCFB to monitor performance and achievements as well as compliance with health and safety and other legislation.

Appendix 4: Responsibilities

Senior Management Responsibilities: Each Dean/Deputy Dean of Academic Centre or Director/Head of Service is responsible for:

- Ensuring that the personal data held by that Academic Centre or Service is kept securely and used properly, within the principles of the UK GDPR and Data Protection Act 2018;
- Advising the Data Protection Officer or delegated representative of the types of personal data held in their School or Service, and of any changes or new holdings;
- Notifying the Data Protection Officer of any instances that could be considered a breach of the legislation;
- Ensuring that any advice, guidance or instruction issued by the Data Protection Officer, or delegated authority in terms of data protection compliance are given due consideration and where appropriate, passed down to team level for action;
- Ensuring that all staff or where appropriate, students receive data protection training; and
- Ensuring that, where necessary, staff are provided with resources required to complete mandatory data protection activities including responding to information rights requests and data protection impact assessments.

Staff Responsibilities: All staff are responsible for:

- Only processing personal data for the purposes explicitly required for their role;
- Ensuring that data they are responsible for is kept securely and protected against unlawful processing, accidental loss, damage or destruction;
- Attending data protection training if any part of their role could involve processing personal data;
- Reporting known or suspected breaches of data protection to their immediate line manager;
- Ensuring that any processing of personal data takes place within the limits of UCFB's Fair Processing Notices and complies with our policies; and
- Notifying the Data Privacy Team, if they wish to use an application, system or service that is not supported by IT Services that will involve the processing of personal data.

Student Responsibilities:

- Students must ensure that all personal data provided to UCFB is accurate and up-to-date. They must also ensure they notify UCFB promptly about changes to any of their data (such as a change of address);
- Students who use UCFB's computing facilities may process personal data as part of their studies. - if personal data is processed, students have a responsibility to ensure that all processing is in line with the data protection principles above; and
- Students who are undertaking research projects using personal data must ensure that:
 - The research has been subject to ethical review and ethical approval has been received;
 - All research participants are informed of the nature of the research and is given a copy of UCFB's Fair Processing Notice and this Data Protection Policy;
 - Where consent of a Data Subject is required for processing, consent must be in writing, freely given, specific, informed, and an unambiguous indication of the Data Subject's wishes;
 - The Data Subject understands that consent can be withdrawn at any time; and
 - All information is kept securely using appropriate technical controls (IT Services can be contacted for guidance).

Appendix 5: Information Rights

The information rights within data protection law are

- The right to be informed;
- The right of access;
- The right to rectification;
- The right to erasure;
- The right to restrict processing;
- The right to data portability;
- The right to object; and
- Rights in relation to automated decision making and profiling.

Where an individual makes a request relating to any of the rights listed above, UCFB will:

- Consider each such request in accordance with all applicable data protection laws and regulations;
- No administration fee will be charged for considering and/or complying with such a request unless the request is deemed to be unnecessary or excessive in nature;
- A response to each request will be provided within 30 days of the receipt of the written request from the Data Subject;
- Appropriate verification must confirm that the requestor is the Data Subject or their authorised legal representative; and
- Data Subjects shall have the right to require UCFB to correct or supplement erroneous, misleading, outdated, or incomplete personal data.

If UCFB cannot respond fully to the request within 30 days, the DPO shall provide the following information to the Data Subject or their authorised legal representative within the specified time:

- An acknowledgement of receipt of the request;
- Any information located to date;
- Details of any requested information or modifications which will not be provided to the Data Subject, the reason(s) for the refusal, and any procedures available for appealing the decision;
- An estimated date by which any remaining responses will be provided;
- An estimate of any costs to be paid by the Data Subject (e.g. where the request is excessive in nature); and
- The name and contact information of the UCFB individual who the Data Subject should contact for follow up.

Appendix 6: Fair Processing Notices

Fair processing notices provide you with information about what an organisation is going to do with your personal data to allow you to decide for yourself if you are happy to give your data to them. UCFB has a range of Fair Processing Notices for different situations as follows. These notices may change from time to time as we evolve how we use your data. If you have any queries you can always contact us via: DataPrivacyTeam@ucfb.ac.uk.

Staff fair processing notice

Who we are

- UCFB act as the Data Controller for the purpose of the Data Protection Act (2018).
- We will make decisions about what personal data we collect from you and how we use it fairly, lawfully and in a transparent manner.
- Our Data Protection Officer can be contacted on DataPrivacyTeam@ucfb.ac.uk.

What we collect from you

- We collect and process your personal and sensitive category data including:
 - Name address and contact details for getting in touch with you;
 - Financial details for payroll and pension purposes;
 - Sensitive data including your ethnicity, declared disabilities and health information for equality monitoring, and our legal obligations;
 - Data relating to your role including data used for performance assessment; and
 - Data relating to any personal devices that you connect to our network.

Lawful basis

- All processing of personal data needs a lawful basis;
- As your employer, our principal lawful basis is the fact there is a contract between you and us for us to provide you with employment; and
- We may process your personal data under a different lawful basis depending on the circumstances of the processing. For example:
 - We will process your personal data where we are legally required to, e.g. we are legally required to ensure you pay your taxes;
 - We will process your personal data for our public tasks, e.g. we will share some personal data with the Office for Students as part of our statutory return; and
 - We will process your personal data based on our legitimate interests, e.g. publicising your work contact details, or as part of a performance appraisal.

What we do with your data

- We collect and use your personal data for the following purposes:
 - To provide you with employment, pay pensions, and other staff service;
 - To meet our legal obligations around taxation health and safety and equality;
 - To meet our statutory obligations as a higher education provider such as submitting our application to join the Office for Students Register; and
 - To fulfil our legitimate interests as a business such as using your data in staff lists, contact directories, or employee appraisals.
- We share your data with other organisations that carry out work on our behalf. These organisations are called Data Processors. We only share the data necessary for them to carry out their tasks and we have a contract with them to limit what they do with your data. Where we share your data outside of the EU, we will do so when we are satisfied that there are the correct safeguards in place.

- We may also share your data with other organisations that use that data for their own purposes, for example, to provide you with a pension. These organisations are also Data Controllers and they will make their own decisions about how they use your data outside of our control.

Your rights

- Everyone has rights about how their personal data is collected, used, stored and managed;
- You can exercise these rights at any time, but not all rights are applicable in every circumstance – for more details contact the Data Privacy Team;
- You have the right to complain to the Information Commissioners Office via ico.org.uk and to seek judicial remedy if you believe we have done something wrong with your data- for more details contact the Data Privacy Team.

Prospective students and Outreach and Access Participant fair processing notice

Our contact details

UCFB is the "Data Controller" for any personal data that we collect, use, store or otherwise process. Any queries relating to Data Protection should be directed to: Data Privacy Team, UCFB, Arch View House, First Way, Wembley, London, HA9 0JD or DataPrivacyTeam@ucfb.ac.uk.

The type of information we have

When you apply to study with us, register for one of our events or open days, take part in an Outreach and Access activity or sign up to hear more about studying with us, we collect the following data about you:

- Your contact details including your name, address, email, contact phone number;
- Geographical information;
- Information on your interests that relate to courses and events or recruitment activities on or off campus; and
- Additional information from Outreach and Access activity, such as your date of birth, gender/sex, postcode, school/college, year group, disability including a learning difficulty or long-term physical or mental health condition, ethnicity information, if you are In Care, estranged from your family, or from a military family.

When you apply to study with us, we will collect the following personal data about you as part of your application:

- personal details (name, address, date of birth);
- phone numbers;
- email addresses;
- identity documents;
- agent information (for those students using an agent);
- gender;
- gender identity;
- photographs;
- financial information;
- academic marks;
- appraisals;
- references;
- disciplinary information;
- health and disability information;
- ethnicity data;
- sexual orientation;
- religious belief data;
- caring responsibilities ;
- personal data that is needed to provide academic and pastoral support; and
- emergency contact details.

Lawful Basis

All personal data that is collected by us, is done so in accordance with the requirements of the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 (DPA), and the Data (Use and Access) Act 2025 (DUAA).

When UCFB processes your personal data, we are required to have a lawful basis for doing so. As a prospective student when you sign up to hear more about studying with us or attend one of our events or open days, our lawful basis for processing your personal data is Legitimate Interest.

As a prospective student, that is applying to study with us, our lawful basis for processing your personal data is a Contractual Obligation. If you accept an offer to study at UCFB, a contract is entered into between you and UCFB. Where we process sensitive category data, such as data relating to ethnicity, religion, or information relating to your health or disability, we are required to rely on a separate lawful basis specifically for that type of personal data. The circumstances for processing will determine the lawful basis chosen. Sensitive category data, in relation to an application to study with us, is processed under legal obligations related to employment, social protection or social security law. We have further obligations under equality legislation, and we may therefore process such information because it is substantially in the public interest to promote equality of opportunity and treatment.

How do we get the information and why do we have it?

We collect personal data about you in the following ways:

- Web forms on uel.ac.uk including registrations for events or requests for more information;
- Direct emails to the Student Recruitment mailbox/email addresses;
- Registrations for events;
- Via tablets at events in an electronic format;
- From Applicants already in our student records system who have applied through UCAS, or directly to UCFB;
- Via our online application process;
- Via surveys and feedback forms.

We will use the personal data that we collect from you for the following purposes and will not use this data for any other purpose without telling you.

- To record and respond to your enquiry or to register and administer your attendance at a Student Recruitment Event;
- To provide communications relevant to becoming a UCFB Student;
- The promotion of our recruitment Open Days and Evenings;
- The promotion of other recruitment initiatives either, on campus, online, on location in the UK or abroad;
- Analysis and reporting of prospective student data and statistics;
- To process your application to study with us, including adding you to our database; and
- If you are a prospective student in our database and make an application to us, we will use the data you provide to match your prospective student record with your application record to ensure the communications we send about the application process and studying with us are relevant.

Data Protection information specific to Outreach and Access interventions:

The outreach and access teams at the UCFB carry out a wide range of outreach interventions that are available to students both locally and across the UK. We also deliver 'in-reach' retention and progression activities for students from underrepresented backgrounds. We ask for specific personal data when participants take part in outreach and access interventions, to show we are meeting our aims of improving participation at higher education level, as well as improving retention and progression whilst UCFB. We want to ensure that we are giving young people from all backgrounds the information that they need to make an informed choice about higher education providers. Collecting personal data allows us to report and monitor this. This is part of government policy to eliminate inequalities in higher education. For further information, please see the [Office for Students website](#).

We collect details of individuals taking part in our activities for the following reasons:

- To plan interventions;
- To monitor participation in interventions;
- To evaluate and report on the impact of these interventions; and
- To understand the student journey through education and progression to higher education/future careers.

The lawful basis to process this data is Public Interest. It is necessary for the outreach and access teams to process your data in accordance with our obligations in line with the aims of the Office for Students. Personal data we ask you for:

- Full name;
- Date of birth;
- Gender/Sex;
- School/College name;
- Year group;
- Postcode;
- Email address;
- Ethnicity information;
- If you have a disability, learning difficulty or long-term physical or mental health condition;
- If you are the first person in your family to obtain a higher education degree;
- If you are In Care (i.e. live with a Carer/s rather than your parent/s for at least three months);
- If you are estranged from your family (i.e. you are not in contact with and not supported by your family); and
- From a military family (i.e. you have a parent/guardian who serves/served in the military).

How we collect your data:

Data will be most commonly requested from students aged 13 years or older (from Year 9 upwards). To process your data, we may use Jisc Online Surveys (or another secure, UK GDPR-compliant form). This tool allows us to collect data and produce graphs for analysis of your responses. Your information will be removed from the online survey tool by March in the following academic year. Your personal details (for example, your name) will be transferred from Jisc Online Surveys (or similar) onto an online database called the Higher Education Access Tracker (HEAT). Data may be collected via paper form which will be kept securely in a locked cupboard and transferred onto HEAT within two weeks upon completion of an intervention. Paper copies are then destroyed using confidential waste bags. Data may be collected via your school, parents or a third-sector organisation, depending on the intervention you are participating in.

How we store your data:

All data is stored in line with the Data Protection Act 2018 (DPA). Student data that relates to outreach and access work is stored in HEAT, who provide a tracking and monitoring service for us. This service is supplied by the University of Kent, it enables us to track the progression of outreach participants into higher education, their attainment in higher education, plus their progression into skilled employment or further postgraduate study. For research and evaluation purposes, we may also share your data with HEAT researchers and the following bodies:

- The Office for Students (OfS);
- The Department for Education (DfE);
- Education and Skills Funding Agency (ESFA);
- The Higher Education Statistics Agency (HESA); and
- The Universities and Colleges Admissions Service (UCAS)

Your data will never be shared unless we are required to do so by law.

How long will your data be kept?

Under 21 years old at the time of first outreach activity: Your data will be retained for 15 years after graduation or until 30 years of age (whichever is greater).

Over 21 years old at the time of first outreach activity:

- Your data will be retained for 15 years after graduation, or for 10 years after your first outreach activity; and
- After this time has been reached, data will be anonymised in bulk at the beginning of the next academic year.

For further information please see [HEAT's data privacy webpage](#).

We will have access to your data if you have previously taken part in an outreach and access event and consented to monitoring and/or being tracked long-term prior to July 2021.

Sharing your information

External Sharing: We may share data about you with third-party processors contracted by UCFB. We use third parties to perform a range of tasks including databases and systems to process enquiries and applications, send email, SMS or video messages, make phone calls, use Live Chat or manage events and webinars. We work with marketing agencies to promote courses and advertise information regarding UCFB. We may work with overseas agents for international recruitment. UCFB takes its obligations with your data very seriously and will ensure that all appropriate safeguards and security provisions are in place and full compliance with its third-party agreements and privacy notice are monitored. For more information on the third-party processors we use, please contact the DataPrivacyTeam@ucfb.ac.uk.

Internal Sharing: When you make an application with us, your personal data will be shared with the departments within the institution that are responsible for processing your application.

Cookies and Analytics: If you visit ucfb.ac.uk, we will send your computer a "cookie", a small text file that resides on your computer's hard drive. Cookies identify a user's computer to our server but in no way gives UCFB access to your computer or any information about you, other than the data you choose to share. The UCFB website uses cookies for collecting user information and allows us to make the website more useful

by tailoring the services we offer from time to time. You can set your browser not to accept cookies, although you may not be able to access all of the features if you do. The website also uses Google Analytics, a web analytics service provided by Google, Inc. Google Analytics sets a cookie in order to evaluate your visit to our website and compile reports and to help us improve the site.

Google stores the information collected by the cookie on servers in the United States. Google may also transfer this information to third parties where required to do so by law, or where such third parties process the information on Google's behalf. Google will not associate your IP address with any other data held by Google. By using the UCFB website, you consent to the processing of data about you by Google in the manner and for the purposes set out above. See [Google's Privacy Policy](#) for more information.

Records Retention

Your personal data will be kept in line with the [UCFB Records Lifecycle Management Scheme](#). This is a large document so, if you have any specific queries, please contact us via: DataPrivacyTeam@ucfb.ac.uk. Your personal data will be kept in line with the Scheme and will be disposed of when:

- We have met our legal retention requirements for your personal data; or
- We no longer have a legitimate reason to maintain that data and it is considered not to contain information which has archival value to UCFB.

How we store your information

All personal data that we process about you will be stored securely and in line with the requirements set out in the UK GDPR. Wherever possible, we will store your data within the European Union (EU) or European Economic Area (EEA). Where this is not possible, and we need to store your data outside of the EU/EEA, we will only do so when we are satisfied that appropriate safeguards are in place.

Your data protection rights

You have rights associated with how your personal data is used and managed. These rights include:

- To be informed what personal data about you UCFB holds and what it is used for;
- To access your personal data;
- To update the personal data UCFB holds about you;
- To be informed how UCFB is complying with its obligations under the Act;
- To complain to the Data Protection Officer or Information Commissioner (ico.org.uk); and
- To have personal data erased where there is no compelling reason for us to keep the data.

These rights are not absolute in every circumstance and several factors such as exemptions in law apply. All requests to exercise any of these rights should be made via:

DataPrivacyTeam@ucfb.ac.uk. Where the processing of your personal data or sensitive personal data/sensitive category data is based only on your consent, you have the right to withdraw your consent at any time by contacting the department or service who obtained that consent or UCFB's Data Protection Officer. Examples of where we can only rely on your consent include marketing and promotions, or research.

If you are unhappy with our handling of your personal data or believe that the requirements of the Act (or any legislation arising directly from it) may not be fully complied with, please contact the Data Protection Officer in the first instance.

Student fair processing notice

Who we are

- UCFB acts as the Data Controller for the purpose of the Data Protection Act 2018 (DPA).
- We will make decisions about what personal data we collect from you and how we use it fairly, lawfully and in a transparent manner.
- Our Data Protection Officer can be contacted via: DataPrivacyTeam@ucfb.ac.uk.

What we collect from you

- We collect and process your personal and special category data including:
 - Name address and contact details for getting in touch with you;
 - Financial details for student fee, loans and grant administration;
 - Sensitive data including your ethnicity, declared disabilities and health information for equality monitoring, and our legal obligations;
 - Data relating to your studies including data used for the formation of your student record; and
 - Data relating to any personal devices that you connect to our network.

Lawful basis

- All processing of personal data needs a lawful basis.
- As an applicant or student, our principal lawful basis is that we are providing you with an education as part of our public tasks.
- We may process your personal data under a different lawful basis depending on the circumstances of the processing. For example:
 - We will process your personal data where we are legally required to, e.g. we are legally required to ensure you pay your fees;
 - We will process your personal data for the purposes of a contract that you have with us, e.g. where you stay in our accommodation or we monitor your attendance;
 - We will process your personal data for our public tasks, e.g. we will share some personal data with the Office for Students as part of our statutory returns; and
 - We will process your personal data based on our legitimate interests, e.g. taking your photo for your student ID card; and
 - In some cases will process your personal data with your consent, e.g. when we send you marketing or promotional material and when we rely on your consent to do this, you can withdraw that consent at any time.

What we do with your data

- We collect and use your personal data for the following purposes:
 - To provide you with education and student support services such as access to the library and information and advice;
 - To meet our legal obligations around payment of fees, health and safety and equality;
 - To meet our statutory obligations as a higher education provider such as supplying your data to the Office for Students; and
 - To fulfil our legitimate interests as a business such as providing your data to UCFB's Students' Union or Alumni Team.
- We share your data with other organisations that carry out work on our behalf. These organisations are called Data Processors. We only share the data necessary for them to carry out their tasks and we have a contract with them to limit what they do with

your data. Where we share your data outside of the EU, we will do so when we are satisfied that there are the correct safeguards in place.

- We may also share your data with other organisations that use that data for their own purposes, for example, to provide you with a Student Loan. These organisations are also Data Controllers and they will make their own decisions about how they use your data outside of our control.

Your rights

- Everyone has rights about how their personal data is collected, used, stored and managed.
- You can exercise these rights at any time, but not all rights are applicable in every circumstance. For more details contact us via: DataPrivacyTeam@ucfb.ac.uk.
- You have the right to complain to the Information Commissioners Office via ico.org.uk and to seek judicial remedy if you believe we have done something wrong with your data. Contact our Data Protection Officer via: DataPrivacyTeam@ucfb.ac.uk in the first instance.

Alumni fair processing notice

Who we are

- UCFB acts as the Data Controller for the purpose of the Data Protection Act 2018 (DPA).
- We will make decisions about what personal data we collect from you and how we use it fairly, lawfully and in a transparent manner.
- Our Data Protection Officer can be contacted via: DataPrivacyTeam@ucfb.ac.uk.

What we collect from you

- We collect and process your personal and special category data including:
 - Name address and contact details for getting in touch with you;
 - Education data;
 - Employment data since you graduated from UCFB, if you choose to provide it;
 - Financial details if you want to make a donation to us or attend a payable event; and
 - Sensitive data including your ethnicity, declared disabilities and health information, if you choose to share it, for equality monitoring and, reasonable adjustment at events. It will not be used for any other purpose.

Lawful basis

- All processing of personal data needs a lawful basis.
- As an alumni, our principal lawful basis is that we are providing you with an alumni service as part of our legitimate interest.
- We may process your personal data under a different lawful basis depending on the circumstances of the processing. For example, we will process your personal data where we are legally required to, e.g. we are legally required to follow health and safety law.
- In some cases will process your personal data with your consent. For example when we send you marketing or promotional material. When we rely on your consent to do this, you can withdraw that consent at any time by getting in touch with the alumni team.

What we do with your data

- We collect and use your personal data for the following purposes:
 - To provide you with an alumni service;
 - To understand your preferences in regards to donating to UCFB;
 - To provide you with updates about UCFB and alumni activities; and
 - To promote opportunities for you to further engage with UCFB.

Your rights

- Everyone has rights about how their personal data is collected, used, stored and managed.
- You can exercise these rights at any time, but not all rights are applicable in every circumstance. For more details contact us via: DataPrivacyTeam@ucfb.ac.uk.
- You have the right to complain to the Information Commissioners Office via ico.org.uk and to seek judicial remedy if you believe we have done something wrong with your data. Contact our Data Protection Officer via: DataPrivacyTeam@ucfb.ac.uk in the first instance.

Appendix 7: Data Sharing and Transfers

UCFB will only share personal or sensitive data where one of the scenarios listed below applies:

- The Data Subject has given consent to the proposed transfer or sharing;
- The transfer or sharing of data is necessary for the performance of a contract with the Data Subject;
- The transfer or sharing is necessary for the implementation of pre-contractual measures taken in response to the Data Subject's request;
- The transfer or sharing is required to fulfil a statutory legal obligation;
- The transfer or sharing is necessary for the conclusion or performance of a contract to be concluded with a third party in the interest of the Data Subject;
- The transfer or sharing is legally required on important public interest grounds.
- The transfer or sharing is necessary for the establishment, exercise or defence of legal claims; and/or
- The transfer or sharing is necessary to protect the vital interests of the Data Subject.

In all cases, such transfers will be subject to appropriate safeguards and will only occur when evidence of such safeguards have been provided. Examples of such safeguards include an information sharing agreement or contractual clauses that legally oblige the recipient to respect data protection law.

Third-party processing

Where third-party processing takes place, the department wanting to share personal data with a Data Processor or other party is responsible for ensuring that the Data Protection Officer (DPO) is aware of the requirements and for implementing any specific measures required to make the sharing lawful and secure. Where the third party is deemed to be a Data Controller: UCFB will enter into, in cooperation with the DPO, an appropriate agreement with the third party to clarify each party's responsibilities in respect to the personal data transferred. Where the third party is deemed to be a Data Processor, UCFB is legally required to enter into a contract for the processing of the personal data. The agreement will require the Data Processor to protect the personal data from further disclosure and to only process personal data in compliance with UCFB instructions. All processing of personal data by a Data Processor acting on behalf of UCFB must be documented and the DPO should be notified about any new processing activities that involve personal data or special category data. This ensures that the relevant contractual clauses are made available before processing commences.