



UCFB* Information Security Policy

Owner:	Director of Transformation, Technology, Facilities and Sport
Author:	Head of Transformation & Technology
Version Number:	4.1
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
Changes to the Policy	We reserve the right to update this policy at any time, and we will notify staff, suppliers, and partners by email when we make any substantial updates

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

1. Who we are

UCFB Campus of Football Business Limited (Company number 07440042) is registered in England and Wales with its registered office being at Arch View House, First Way, Wembley, London, HA9 0JD and is referred to as “UCFB” in this Notice. UCFB has appointed a designated Data Privacy Team, which is responsible for overseeing questions in relation to this Privacy Notice. If you have any questions about this Privacy Notice, including any requests to exercise your legal rights, please contact the Data Privacy Team via e-mail at: dataprivacyteam@ucfb.ac.uk or via post to: Data Privacy Team UCFB, Arch View House, First Way, Wembley, London, HA9 0JD.

You have the right to make a complaint at any time to the Information Commissioner’s Office (ICO), the UK supervisory authority for data protection issues (www.ico.org.uk). UCFB welcomes the opportunity to resolve concerns directly in the first instance.

2. Purpose of this Policy

This Policy sets out our commitment to and minimum standards for managing and controlling information security risks. Detailed requirements are set out in supporting policies and procedures within the group information security and data governance policy framework (see Section 16 (below)).

4. Policy Context

4.1. UCFB Business Context

Information that is processed (collected, analysed, stored, communicated and reported upon) by UCFB may be subject to theft, misuse, loss or corruption. Information may be put at risk by poor education and training, and the breach of security controls. Information security incidents can give rise to embarrassment, financial loss, non-compliance with standards and legislation as well as possible judgements made against the company. Ensuring that the data and information relating to students and staff is processed securely is of the utmost importance to the us. Any significant failure in our security procedures and controls could, ultimately put at risk our ability to continue to attract and retain high calibre students and staff.

4.2. Regulatory Context

A key principle of the UK General Data Protection Regulation (GDPR) is that personal data must be processed securely using ‘appropriate technical and organisational measures’. This requires UCFB as a data controller processing personal information about students as well as data relating to staff members to implement a combination of organisational policies, technical and physical controls and procedures to protect the data we hold and process.

5. Scope

This Policy and its supporting controls, processes and procedures apply to all:

- Information used at UCFB, in all formats, whether held electronically or in physical copy;
- Data processed by UCFB relating to prospective applicants, current and former students (“Students”);
- All UCFB employees, workers and contractors (“Staff”); who have access to UCFB information, data, and systems;

- Any third parties that provided goods and services to us (“Suppliers”) and who are given access to or may come into contact with UCFB information, data and systems; and
- All partners who provided data to or share data with UCFB to support our business activities (“Partners”).

6. Roles & Responsibilities

6.1. Responsibility for Information Security

Responsibility for Information Security is set out in Section 7 of the [UCFB Data Protection Policy](#).

6.2. UCFB Data Privacy Team

To support the effective implementation, continuous improvement, and effective operation of the important data governance controls across the institution, the UCFB Data Privacy Team has been established with cross-functional representation. This Team will:

- Identify and assess information security risks and define the strategy and direction to ensure these risks are mitigated;
- Monitor compliance with UCFB’s security policies and the associated supporting controls, and report the levels of compliance to the Executive Leadership Team periodically; and
- Implement and maintain the information security and data governance awareness programme for all staff.

7. Policy Application

UCFB operates a set of information governance controls to ensure that:

- Authorised users can securely access and share information in order to perform their roles;
- Physical, procedural, and technical controls balance user experience and security;
- Contractual, legal, and regulatory obligations relating to information security and data protection are met;
- Individuals accessing our information are aware of their responsibilities; and
- Incidents affecting our information are resolved and learnt from to improve our controls.

8. Information Governance Policy Framework

A set of associated policies relating to controls, processes, and procedures have been defined in support of this Policy and its stated objectives. These policies constitute our information governance policy framework.

9. Access Controls

Access to all information must be controlled and be driven by business requirements. Access must be granted to staff and suppliers according to their role and only to a level which enables an individual to carry out their duties. Specific controls must be implemented for staff with elevated privileges, to reduce the risk of negligent or deliberate system misuse. Elevated privileges relate to staff members who, by virtue of function, and/or seniority, have been allocated powers within the computer system, which are significantly greater than those available to the majority of staff.

10. Supplier Relationships

Our information security requirements must be considered when establishing relationships with new suppliers, to ensure that assets accessible to or shared with suppliers are protected appropriately. Contractual protections must be included within any statement of services, and active management of suppliers to both ensure the goods and services contracted for are being delivered and that any UCFB information and data is being handled and processed securely.

11. Information Security Incident Management

An information security incident is a suspected, attempted, successful, or imminent threat of unauthorized access, use, disclosure, modification, or destruction of UCFB information. Actual or suspected breaches of information security must be reported and investigated. These should be reported to the UCFB Data Privacy Team, via: DataPrivacyTeam@ucfb.ac.uk. Examples of information security incidents that should be reported include:

- Computer system intrusion;
- Unauthorized or inappropriate disclosure of sensitive UCFB data;
- Unauthorised changes to computers or software; and/or
- Loss or theft of computer equipment or other data storage devices and media (e.g., laptop, USB drive, personally owned device used for UCFB work) used to store private or potentially sensitive information.

12. Business Continuity & Disaster Recovery

UCFB has arrangements in place to protect critical business processes from the effects of major failures of information systems or disasters, and to ensure their timely recovery is aligned to the needs defined by the business functions. Business Continuity Plans are maintained and tested in support of this Policy.

13. Privacy by Design

UCFB is committed to the continued improvement of its information governance system. To support this, all new projects and initiatives commissioned by UCFB will be subject to a Privacy Impact Assessment (PIA). This supports staff in understanding their data and information requirements and ensures security-related issues are considered at the start of any project or activity, ultimately leading to higher quality, faster project delivery and continued legal and regulatory compliance by preventing data from being collected and/or processed inappropriately. The UCFB Data Privacy Team is responsible for supporting the PIA process.

14. Policy Exceptions

Requests for exceptions to this Policy or any of its supporting policies, processes, procedures and controls must be submitted to the UCFB Data Privacy Team for review and approval. All exception requests (approved or rejected) will be reported to the Executive Leadership Team periodically.

15. Failure to Comply

Poor or inappropriate behaviour by staff during the collection, processing or disposal of UCFB information and data relating to students and staff, as well as any other confidential or commercially sensitive information held by the institution will be treated with the

utmost seriousness and may result in disciplinary action. In the most serious circumstances, where an individual is found to have wilfully misused personal and sensitive data, a criminal offence may have been committed and those individuals may become personally liable to prosecution. Poor or inappropriate behaviour by suppliers during the collection, processing or disposal of information and data relating to our students and staff, as well as any other confidential or commercially sensitive information held by the company could be treated as a breach of contract and, in the most serious circumstances, result in contract termination and possible redress for any financial costs incurred as a result by UCFB.

16. Related Policies and Procedures

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