Fairfield School of Business

# Data Protection Policy

| | |
|---|---|
| **Version:** | **3.6** |
| Category: | Policies - Statutory and Compliance |
| Owner(s): | Head of Registry; Legal Counsel |
| Approved by: | The Board of Governors |
| Access: | **Public** – Anyone can view this document |
| Scope: | This policy applies to all staff (including contractors and volunteers), students and visitors at Fairfield School of Business (FSB) |

## Contents



## Purpose

This policy sets out the obligations of Fairfield School of Business ("FSB"), a company registered in the UK (number 05849002), whose registered office is at **Office 2, First Floor, Memo House, Kendal Avenue, London, England, W3 0XA**

FSB's Data Protection Policy has been developed with reference to EU Regulation 2016/679 *General Data Protection Regulation ("GDPR")*; whist companies that operate within the UK are (as of January 2021) no longer subject to EU regulation, the GDPR has been incorporated into UK data protection law as the UK GDPR, which sits alongside an amended version of the Data Protection Act (2018).

FSB's appointed Data Protection Officer is:

**Bulletproof Cyber Limited (Data Protection Officer)**

Bulletproof HQ, Unit J, Gateway 1000,
Whittle Way, Stevenage, Herts,
SG1 2FP

+44 (0) 1438 532 916
consulting@bulletproof.co.uk

# 1. Introduction

1.1. Fairfield School of Business ("FSB") obtains, uses, stores and otherwise processes personal data relating to potential staff and students (applicants), current staff and students, former staff and students, current and former contractors, website users and contacts, collectively referred to in this policy as **'data subjects'**. When processing personal data, FSB is obliged to fulfil individuals' reasonable expectations of privacy by complying with relevant data protection legislation ('data protection law').

1.2. '**Personal data'** is recorded information that relates to a living person that can be associated with that person, either from other information in the possession of the organisation holding the data or by cross referencing to information held by a third party. This includes expressions of opinion about the individual and indication of any intentions of the Data Controller or any other person in regard to the individual. Recorded information can be stored electronically or in a manual filing system.

1.3. Examples of Personal Data include:

- Name, home and work addresses
- Date of Birth
- National insurance and passport numbers
- Bank account or credit card details
- Insurance policy details
- Employment records
- Education history
- Images caught on close circuit television (CCTV)
- Student record information
- Student exam results

1.4. To comply with the law, such personal data must be collected and used fairly, stored safely and not disclosed to any other person unlawfully. The principles to ensure that personal data is processed properly, and which FSB follows to ensure it complies with the legislation, are set out in the General Data Protection Regulations (the GDPR), available on the Information Commissioner's Office website (https://ico.org.uk/).

**Under the GDPR, all Personal Data shall:**

1.4.1. be processed fairly and lawfully,

1.4.2. be obtained for a stated purpose(s) and not processed for anything other than the stated purpose(s) and for archiving purposes in the public interest, scientific or

historical research purposes, or statistical purposes,

1.4.3. be adequate, relevant and not excessive for the purpose for which it was obtained,

1.4.4. be accurate and be kept up to date, and if inaccurate be rectified or erased without delay,

1.4.5. except where anonymised so that the individual cannot be identified, shall not be kept for longer than is necessary for the purpose for which it was obtained,

1.4.6. processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

1.5. FSB will ensure that these principles are always followed. Therefore, through appropriate management and strict application of criteria and controls, FSB will process data only as set out in this policy and the FSB Privacy Notice.

## 2. Your rights

2.1. UK Data Protection law secures the following rights provides for individuals:

- 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
- Rights in relation to automated decision making and profiling.

2.2. Further information on how these rights can be found here: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/

## 3. How we use your data

3.1. FSB may use and process personal data (including Special Category data and criminal offence data) both during and after individuals have worked or studies at FSB. Special Category data includes information held by FSB as to your physical or mental health or

condition, your racial/ethnic origin, sexual orientation/sex-life, political views, or religion. Criminal offence data includes information on the commission or alleged commission of any offence by you and any proceedings for an offence committed or alleged to have been committed by you (including the outcome or sentence in such proceedings).

3.2. We may obtain the following categories of personal data from third-parties:-

- Identifying data *e.g. usernames, names, email addresses*
- Tracking data *e.g. attendance records taken by contractor lecturers*
- Financial data *e.g. payment and student finance data collected by contractor finance staff*
- Medical and health information *e.g. sick notes*
- Professional information *e.g. employer or past academic references, academic record information for admissions purposes*
- Criminal data *e.g. enhanced DBS checks for health and social care courses*

3.3. FSB processes personal data, including Special Category Data for the purposes set out in our Privacy Notice. The processing of your personal data for the below purposes is required for the performance of this contract between you and FSB, for FSB to meet its regulatory obligations and for FSB's legitimate interests including marketing, quality assurance, and ensuring safety and security of staff and students. We may also ask for your consent for participation in some marketing activities (e.g. subscribing to marketing information along with our newsletter). If so, you have the right to withdraw such consent at any time.

3.4. The purposes for which FSB may process personal data (including Special Category data) include:

- the administration of your enrolment on and participation on a course, including the administration of examinations, the issue of results and certificates in connection with the course and (where applicable) the provision to your employer or other sponsor/corporate sponsor information about your attendance and performance on a course, and DBS checking where required for a course,
- the provision of FSB services and facilities to you and the protection of your health, safety and welfare whilst at FSB,
- the issue and operation of FSB's ID card in accordance with the conditions of the Student enrolment terms and conditions,
- the collection of tuition fees and other FSB fees,

- equal opportunities monitoring,
- arrangement and marketing of alumni activities,
- the provision of references about you,
- the provision of information to any regulator, government body or agency,
- for safety purposes, and
- the provision of information (to the Higher Education Statistics Agency, HESA[1]) as part of FSB's statutory external returns to the OfS

3.5. HESA information including linked data is used for four broad purposes: public functions, administrative uses, HESA publications and Equal opportunity, research, journalism and other processing in which there is a legitimate interest. For more information see the HESA Collection Notice on http://www.hesa.ac.uk/fpn

3.6. In some circumstances, it may be necessary for FSB to transfer your personal data to a country outside the European Economic Area (for example, if that is your country of origin). Such a transfer will only be made for the purposes specified above.

3.7. You should be aware that countries outside the EEA may not offer data protection law equivalent to that applicable in the United Kingdom and you consent to the transfer of data in these circumstances and for those purposes. Where we make such a transfer to a country that does not provide the same level of data protection as the UK, we will put appropriate measures in place to ensure your information is protected.

3.8. In some circumstances your personal data will be processed by a third party on our behalf – e.g. a work placement provider, a student recruitment agency, or contractor lecturing or administrative staff. Any such processing will only be done under a GDPR compliant processor contract requiring the third-party to only process the data in accordance with our written instructions.

3.9. FSB collects, processes, and stores criminal offence data about past convictions, including enhanced DBS check reports from APCS, details of unspent convictions, and full DBS certificates. This may be required for performance of your contract of enrolment with FSB, and the legitimate interest of protecting the safety of our staff and students. We do not keep a comprehensive record of criminal offence data.

3.10. Your data will be received by the following categories of third-party recipients:

- awarding bodies
- regulators and funding agencies

[1] HESA - Experts in higher education data and analysis

- debt recovery agencies instructed to recover outstanding fees
- contractor staff
- partner course and skill providers e.g. Careers Group, Learn Direct, Trainimaster
- professional advisors e.g. our accountants, solicitors, quality assurance consultants, our DPO
- public authorities, statutory or regulatory bodies and law enforcement e.g. HESA, the police, UKVI.

3.11. FSB may make video and/or audio recordings of face-to-face and online lectures for training and quality monitoring purposes, which may include students' contributions to classroom discussions and expressions of opinion. These recordings may also be used by FSB for investigating suspected instances of misconduct or breaches of security.

3.12. Further to 3.11., in some circumstances, FSB may wish to use data in the form of photographs, or video or audio recording, of classroom situations as part of general marketing materials for example in FSB's annual report, prospectus or course materials. Video and audio recordings and any personal data alongside them will only be used in this way with your explicit consent, which you have the right to withdraw at any time.

3.13. If FSB does not process your data fairly, you may lodge a complaint with the Information Commissioners Office (ICO) here: https://ico.org.uk/concerns/handling/ within 3 months of your last contact concerning the matter with FSB (or such other time limit as the ICO from time to time specify).

## 4. Confidentiality

4.1. All personal information collected and held by FSB staff will be processed with the due care and discretion, so as to comply with applicable data protection law.

4.2. In most circumstances, personal information is treated as confidential, but members of staff may have legitimate reason to share information relating to students' enquiries or circumstances with colleagues or with FSB's senior management so as to discharge its contract to deliver educational services, or where this may in the vital interests of the data subject.

4.3. If such discussions take place as per 4.2, this will usually be for the sole purpose of determining a best course of action. Whenever possible, any such discussion between FSB staff will take place without the use of information that would directly identify the data subject.

## 5. Staff responsibilities

5.1. Staff whose work involves the use of personal data are responsible for ensuring that:

- any personal data which they hold whether electronically or in hard copy is kept securely, including using password protection on computer files,
- personal data is not disclosed by them either orally or in writing, to any unauthorised third party,
- the personal data is accurate and kept up to date, held for the appropriate length of time and destroyed confidentially when/if no longer needed, and
- they do not access any personal data which is not necessary for carrying out their work.
- report any data breach to the DPO within 48 hours where feasible, to allow to FSB to comply with its obligation to record all data breaches, and to report a data breach to the ICO within 72 hours.

5.2. Managers have an additional responsibility to ensure that their staff are aware of the data protection principles and know how to correctly process personal and sensitive personal data as part of their work.

## 6. Student responsibilities

6.1. It is student's responsibility to inform FSB if their personal details require updating. We will provide an annual opportunity for a student to check their data through the registration process.

6.2. We also collect, at registration, the contact details of a person nominated by student for emergency contact purposes. A student must notify them that we are holding this data which will only be used in an emergency.

## 7. Students with disabilities or dyslexia

7.1. If a student has declared a disability or dyslexia, FSB is legally required under the Equality Act 2010 to make appropriate and reasonable adjustments in order to help such student to participate to the fullest extent possible in the educational opportunities provided by FSB. Information about the student situation and requirements will be limited to that necessary to assure that appropriate adjustments can be made to help the student gain maximum benefit from their course of study. Any information will normally

only be passed to others with student's agreement.

## 8. Subject Access Requests

8.1. Data subjects are entitled to request a copy of the data FSB holds about them. Any person who wishes to exercise this right should complete the '*Subject Access Request'* form available from the Student Portal and submit it to the Registry, however a request can be made verbally or through any medium to any member of staff at FSB.

8.2. FSB will comply with requests for access to personal data as quickly as possible but will ensure that it is provided within 28 calendar days of receipt of the request. FSB can extend the time to respond by a further two months if the request is complex or it has received a number of requests from the student. FSB will inform the student within 1 month of receiving their request and explain why the extension is necessary.

## 9. Retention of records

9.1. Application data will be retained for 6 months from the date of the application if enrolment is not successful. We will retain a full student record for 6 years after a student has left FSB so that we can fulfil a duty to provide details of your education and references when asked to do so. After this time, we will keep enough data about a student to be able to confirm the qualifications achieved whilst at FSB.

## 10. Key contact details

- **Fairfield School of Business Ltd (Data Controller)**

  Office 2, First Floor, Memo House, Kendal Avenue, London, England, W3 0XA
  info@fairfield.ac

- **FSB Registry (for students' data Subject Access Requests)** registry@fairfield.ac

- **Human Resources (for employee data Subject Access Requests )** hr@fairfield.ac

- **Bulletproof Cyber Limited (Data Protection Officer)**

  Bulletproof HQ, Unit J, Gateway 1000,
  Whittle Way, Stevenage, Herts, SG1 2FP

+44 (0) 1438 532 916
consulting@bulletproof.co.uk

## Appendix A: Subject Access Request Form

# Subject Access Request (Page 1)

**Purpose of this form:**

It is not mandatory to use this form, but it will help us to give a timely and accurate response to your subject access request as required in the General Data Protection Regulation.

Please complete the table below and return the form by post to Fairfield School of Business, First Floor Memo House, Kendal Avenue, Park Royal, W3 0XA, marked for the attention of Registry: registry@fairfield.ac (if you are a student), or HR: hr@fairfield.ac (if you are an employee of FSB or a contractor).

**About you**

| | |
|---|---|
| Title | |
| Forename(s) | |
| Surname | |
| Other names we may know you by | |
| Any reference numbers or information that will help us locate the information we hold on you | |

**How may we contact you? (Provide at least one way)**

| | |
|---|---|
| Telephone | |
| Email address | |
| Postal address | |

**Proving your identity**

We are required to try and verify that you are the person named above. We may ask for one of the following documents – Please tick the ones you could supply:

- ☐ A copy of your passport
- ☐ A copy of your European driving licence
- ☐ A copy of a recognised photo ID
- ☐ An original utility bill issued in your name

# Subject Access Request (Page 2)

**Your request**

Please outline the information to which you wish us to provide access:

# (Guidance on Making a Subject Access Request)

**What are your rights?**

The Data Protection Act 2018 gives individuals a right of access to the personal data which organizations hold about them, subject to certain exemptions (see 2. below). Requests for access to personal data are known as Subject Access Requests. This guidance explains process as how to submit a subject access request to FSB, how FSB will handle request, and right to complain if dissatisfied.

If a SAR request is made to FSB, individuals are an entitled to be told whether FSB hold any data about them. If FSB does, the staff member has a right:

- To be given a description of the data, the purposes for which the data are being processed, and those to whom the data may have been disclosed;
- To be given a copy of the data in an intelligible form, with any unintelligible terms explained;
- To be provided with any information available to FSB about the source of the data; and
- If staff member specifically request it, to be given an explanation as to how any automated decisions taken about them has been made. These rights apply to electronic data, and to data in "manual" (i.e. non-electronic) formats, subject to certain limitations in regard to unstructured manual data (see 3. below). Further information about staff rights under the Data Protection Act is available on the website of the Information Commissioner (www.ico.gov.uk).

**What are the exemptions?**

The Data Protection Act includes various exemptions which specify the circumstances in which an organization can refuse to provide access to personal data. The most likely situations in which FSB could lawfully refuse a subject access request are where:

The release of the data would jeopardise the prevention or detection of crime, or the apprehension or prosecution of offenders;

- You have requested access to an examination script, other than examiners' comments;
- You have requested data contained in a confidential reference provided by FSB;
- Staff member requested data which record FSB's intentions in relation to any negotiations with that staff member, and the release of the data would prejudice the negotiations;
- The data is covered by legal professional privilege.

If FSB withholds data from staff member or anyone as a result of an exemption under the Data Protection Act, FSB will explain why the data have been withheld and the relevant exemption, unless doing so would itself disclose information which would be subject to the exemption.

The Data Protection Act allows FSB to refuse to provide staff member or anyone with a copy of staff member data if the effort in doing so would be disproportionate, or if the same or similar data have already been provided to them or their associates or anyone in context to the staff member and a reasonable interval has not elapsed since staff member or anyone on their staff member's behalf to previous subject access request. In addition, if FSB reasonably requires further information from a staff member in order to locate the data which the staff member had requested, and FSB has informed staff member or their representatives of this, FSB does not required to comply with request until the staff member or their representative supply FSB with the information.

FSB has to protect the Data Protection rights and other legal rights of other individuals when responding to subject access requests. Information which does not relate to a staff member may be 'blanked out' or edited out, particularly if it relates to other individuals. Sometimes FSB may not be able to release data relating to staff member or their representatives because doing so would also reveal information about other persons who have not consented to their data being released, and it would not be reasonable in the circumstances to release the data without their consent. In such cases, staff member or their representatives will be informed that data about the staff member has been withheld and the reasons for doing so.

**What happens after the request is received?**

FSB will send an acknowledgement of request as soon as possible. This will indicate the deadline by when FSB will send a response. FSB may also ask to provide further information or clarification if FSB requires it to process request and may contact again for additional information or clarification if necessary. After the FSB receives request, FSB must consider it and respond to it. FSB will respond as soon as possible, and in all cases within 1 calendar month of receipt of the request. If FSB reasonably require further information to locate the data which has been requested, FSB will inform you as soon as possible, and the 30-day deadline will commence from the date when we receive the information from the staff member or their representatives. FSB will normally send the data electronically through a shared OneDrive folder, unless FSB agree with staff member or their representatives that the data can be supplied in a different format.

The data may take the form of photocopies, printouts, transcripts or extracts, or a combination of these, depending on what is most appropriate in the circumstances. Although staff member or their representatives do not have a right to inspect original documents, FSB may offer this to staff member or their representatives where supplying staff member or their representatives with copies of the data would involve disproportionate effort.

If FSB holds no data about staff member, staff member or their representatives will be informed of this. Staff member or their representatives will also be informed of any cases where data about staff member has been withheld and the reasons for this, including the relevant exemptions (see above), unless doing so would itself reveal information which would be subject to an exemption.

**Can I appeal?**

You can ask for an internal review if FSB refuses your subject access request or you are dissatisfied with the handling of staff member request. Appeals should be sent in writing to the CEO, at the following address:

**F.A.O Chief Executive Officer**
**Fairfield School of Business**

Memo House, 1st Floor, Kendal Avenue,
London, W3 0XA
+44 (0) 208 7953 863
info@fairfield.ac

The CEO will acknowledge appeal within seven working days, and will consult with the Data Protection Officer. A response will be sent to you within 28 calendar days of receipt of appeal. If it includes a decision that data should be released, the information will be provided as soon as possible. Staff or their representatives can also ask the Information Commissioner for an assessment as to whether FSB has processed data in accordance with the Data Protection Act. The Commissioner can be contacted at the following address:

**Information Commissioner**

Wycliffe House Water Lane
Wilmslow Cheshire
SK9 5AF
United Kingdom

## Version Tracking:

| Version | Author / revisions by | Changes summary | Approved by | Date |
|---|---|---|---|---|
| 1.0 – 3.1 | Data Protection Officer<br>Legal Advisor<br>Executive Committee | Original version and subsequent updates. | Executive Committee | Sep 2016<br>Sep 2017<br>May 2018<br>Sep 2018 |
| 3.2 | Risk and Audit Manager<br>Legal Advisor | Factual updates: Change of data protection officer; Reviewed by the Publications Committee. | Board of Governors | May 2020 |
| 3.3 | Risk and Audit Manager<br>Legal Advisor<br>Head of Registry | Annual review and update. Addition of clause in recording lectures. Expanded definition of personal data. Addition of SAR form template | Board of Governors | October 2020 |
| 3.4 | Quality Manager<br>Legal Counsel | New formatting and version control applied. | Board of Governors | October 2022 |
| 3.5 | Quality Manager<br>CEO | Contact information updated. | Board of Governors | September 2023 |
| 3.6 | Quality Manager<br>CEO | Minor updates to phrasing to align with legal definitions. Amended registered address | Board of Governors (C.A.) | July 2024 |
| | | Review date extended | Board of Governors | October 2024 |

**Date of next review:** September 2026