



Data Protection Policy

POLICY / DOCUMENT PURPOSE STATEMENT

The purpose of this policy is to highlight the college's responsibility with regards to collecting, storing and processing personal data. The policy also highlights individuals' rights with regards to the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, the Privacy and Electronic Communications Regulations (PECR) and the Data (Use and Access) Act 2025 (DUAA).

APPLICATION

The policy applies to all students, staff, governors, temporary members of staff & external providers.

INTERPRETATION

Further guidance on the use or interpretation of this policy may be obtained from the Data Protection Officer.

LINKS WITH OTHER POLICIES / DOCUMENTS

Data Archiving & Retention Policy
Freedom of Information Policy
Rights of Individuals Policy & Procedure
Data Breach Notification Policy & Procedure
Disciplinary Policy & Procedure
Professional Code of Standards
Safeguarding Policy
CCTV Code of Practice

Version number	7
Author	Andy Gazey
Owner / Area	Andy Gazey/ Operations
Date of implementation	20/07/2018
Review date	20/07/2020
Ratified / Authorised by	Operations Committee 13.11.2019
Review Frequency	2 Years
Review Ratified/Approved Date	Operations Committee 14.06.2023
Review Date	August 2026
Target Review Ratified/Approved Date	Operations Committee 14.11.2026
Next Review Due	November 2028

1. Introduction

- 1.1.** The College acts primarily as a Data Controller and, in limited circumstances, may act as a Data Processor where it processes personal data on behalf of another organisation.
- 1.2.** In this role, Fircroft College needs to keep certain information about staff, students and other users. It is necessary to process information so that staff can be recruited and paid, courses organised and statutory obligations to funding bodies and government are complied with. Any information must be used fairly, stored safely and not disclosed to any other person unlawfully. To do this, the College must comply with the Data Protection Principles which are set out in the Data (Use and Access) Act (DUAA), and UK GDPR. In summary these state that personal data shall:
 - 1.3.** Processed lawfully, fairly and in a transparent manner in relation to individuals;
 - 1.4.** Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
 - 1.5.** Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
 - 1.6.** Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
 - 1.7.** Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the UK GDPR in order to safeguard the rights and freedoms of individuals;
 - 1.8.** 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;
 - 1.9.** Personal data transferred outside the United Kingdom will only occur where appropriate safeguards, adequacy regulations or approved transfer mechanisms are in place.
 - 1.10.** Article 5(2) of the General Data Protection Regulation requires that
 - 1.11.** “The controller shall be responsible for, and be able to demonstrate, compliance with the principles.”

1.12. All staff, Governors and students who process or use any personal information must ensure that they follow these principles at all times. Fircroft College has developed this Data Protection Policy to ensure that staff adhere to the UK GDPR principles at all times.

1.13 The College may rely on lawful bases permitted under UK GDPR including consent, contract, legal obligation, vital interests, public task, legitimate interests and recognised legitimate interests where permitted by legislation. Consent is not the primary lawful basis for most College processing activities.

2. Status of the Policy

2.1. This policy does not form part of the formal contract of employment, but it is a condition of employment that staff will abide by the rules and policies made by the College. Any failure to follow the policy can therefore result in disciplinary proceedings.

2.2. Any member of staff who considers that the policy has not been followed in respect of personal data about themselves should raise the matter with the designated Staff Data Controller (Stephen Hayden, Director of Finance) initially. If the matter is not resolved it should be raised as a formal grievance.

2.3 Personal Data is defined as information about a living person which is kept in a manual or computerised system to identify an individual. This information is protected by UK GDPR.

2.4 "Special Category Personal Data" includes personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data used for identification, health data, and data concerning a person's sex life or sexual orientation.

2.5 The College will have records of internal communications which are relevant to an individual's relationship with the College including information concerning performance and conduct issues. Such records should comply with the principles outlined under UK GDPR

3. Individuals Rights Under UK GDPR

3.1.1. The College is dedicated to ensuring individuals rights under UK GDPR are upheld. Any information the College holds about an individual will be available under UK GDPR. These rights are:

3.1.2. The right to be informed regarding the information collected and processed in respect to that individual.

3.1.3. The right of access allows an individual to request through a Subject Access Request (SAR) any personal or supplementary information held by the College.

3.1.4. The right to rectification allows an individual to request any incorrect or incomplete information to be corrected.

3.1.5. The right to erasure or the right to be forgotten as it is also known allows an individual the right to request that their personal data is removed or deleted from

file. The College can refuse this request if deleting this information would be in breach of contract compliancy or legislation.

3.1.6. The right to restrict processing allows an individual to request that the information stored by the College will be held for the purpose of compliancy to a contract but will not be processed further.

3.1.7. The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services. It allows them to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability. The College will work to facilitate this right where applicable and not in violation of contractual guidelines.

3.1.8. The right to object allows individuals the ability to request that their personal information is not processed for purposes of scientific or historical research, data profiling or direct marketing.

3.1.9. Finally, Where the College uses profiling, artificial intelligence or automated decision-making that significantly affects individuals, appropriate safeguards will be implemented including:

- meaningful information regarding the logic involved;
- the right to obtain human review;
- the right to contest decisions;
- processes to ensure fairness and non-discrimination.

3.2. For more information regarding individuals rights please see the colleges 'Rights of Individuals Policy and Procedure'.

4. Children's Data Protection

The College currently does not enrol students under the age of 18.

The College recognises that children and young people require additional protection when their personal data is processed.

When processing personal data relating to learners under the age of 18, the College will take their rights, vulnerabilities and best interests into account.

5. Responsibilities of Staff

5.1 Staff are responsible for

5.1.1 Checking that any information that they provide to the College in connection with their employment is accurate and up to date.

5.1.2 Informing the College of any errors or changes. The College cannot be held responsible for any errors unless the staff member has informed the College of them.

5.2 If and when, as part of their responsibilities, staff collect information about other people, (e.g. about students' course work, opinions about ability, references to other academic institutions, or details of personal circumstances), they must comply with the principles laid down by the UK GDPR.

5. Governance

Governing Body

Responsible for ensuring adequate data protection arrangements exist.

Principal

Responsible for operational compliance.

Senior Information Risk Owner (SIRO)

Responsible for information risk management

Data Protection Officer (if appointed)

Responsible for advice, monitoring and liaison with the ICO.

Operational Leads/Managers

Responsible for compliance within their areas.

6. Data Security

6.1 All members of staff are responsible for ensuring that:

6.1.1 Any personal data which they hold is kept securely.

6.1.2 Personal information is not disclosed either orally, (including by telephone) or in writing or accidentally or otherwise, to any unauthorised third party.

6.1.3 Personal information is not disclosed without the express authorisation of the Principal or Staff/Student Data Controller.

6.2 Staff should note that unauthorised disclosure will usually be a disciplinary matter, and may be considered gross misconduct in some case.

6.3 Personal information should be:

6.3.1 Kept in a locked filing cabinet; or

6.3.2 in a locked drawer; or

6.3.3 If it is computerised, is password protected or securely stored with two-factor authentication enabled.

7. Remote Access

7.1 Any remote access using either dial-in, VPN, or any other remote access to the organisational network must be reviewed and approved by the appropriate supervisor. All staff, by default will have account settings set to deny remote access. Only upon approval will the account settings be changed to allow remote access.

7.2 Remote Access is supported with two-factor authentication and must be enabled before remote access can occur.

8. Student Obligations

8.1 Students must ensure that all personal data provided to the College is accurate and up to date. They must ensure that changes of address, etc are notified to the student admissions office/other person as appropriate.

Students who use the College computer facilities may, from time to time, process personal data. If they do, they must notify the designated Student Data Controller (Information Systems & IT Manager). Any student who requires further clarification about this should contact the designated Student Data Controller.

9. Rights to Access Information

9.1 Staff, students and other users of the College have the right to access any personal data that is being kept about them either on computer or in certain files. Please see the college's 'Freedom of Information Policy' or see the HR Manager for the "Access to Personal Information Form" (Appendix 1) form.

9.2 Requests are normally free of charge. Fees will only be charged where permitted under data protection legislation, such as manifestly unfounded or excessive requests.

9.3 The College will undertake reasonable and proportionate searches when responding to Subject Access Requests.

10. Publication of Fircroft College Information

10.1 UK GDPR gives a general right of public access to all types of recorded information held by "public authorities." The College falls under this definition of a public authority and is therefore covered by the Act. Any information that is already in the public domain is exempt from the Acts. It is the College policy to make as much information public as possible.

11. Special Category Data Consent

Processing Special Category Information

11.1 Personal data will only be processed where the College has identified a lawful basis under Article 6 UK GDPR. These may include consent, contract, legal obligation, vital interests, public task and legitimate interests.

11.2 Certain categories of personal data require an additional condition for processing under Article 9 UK GDPR and, where applicable, Part 1 of Schedule 1 of the Data Protection Act 2018. These will be investigated as required by the College.

11.3 Sometimes it is necessary to process information about a person's health, criminal convictions, race, gender and family details. This may be to ensure the College is a safe place for everyone, or to operate other College policies, such as the sick pay policy or Single Equality Scheme. More information about this is available from the Data Controller.

11.4 Criminal offence data is subject to separate protections under Article 10 UK GDPR and Part 3 of the Data Protection Act 2018.

13. The Data Controller and Data Processor the Designated Data Controller/s

13.1 The College acts as a Data Controller and, where applicable, a Data Processor in accordance with UK GDPR and the Data Protection Act 2018. The Governing Body retains overall accountability for data protection compliance

13.2 However, there are designated Data Controllers dealing with day to day matters. The first point of contact for enquirers is:

Stephen Hayden, Director of Finance, Fircroft College, 1018 Bristol Road, Selly Oak, Birmingham B29 6LH, telephone 0121 472 0116.

Who may either deal with the enquiry or refer it to another designated data controller if applicable.

14. Use of CCTV.

14.1 The College uses CCTV for the prevention and detection of crime and for the security and safety of students, staff, college users and protection of the College premises. The use of CCTV system is subject to the College's CCTV and Audio Recording Policy

15. Examination Marks

15.1 Students will be entitled to information about their marks for both coursework and examinations. However, this may take longer than other information to provide. The College may withhold certificates, accreditation or references in the event that the full course fees have not been paid, or where college resources such as books and equipment have not been returned to the College.

16. Retention of Data

16.1 The College will keep some forms of information for longer than others. Due to storage limitations, information about students cannot be kept indefinitely. Please see a copy of college 'Data Archiving & Retention Policy' for reference.

16.2 After the retention date has been reached any confidential information will be disposed of in accordance with existing arrangements.

17. Reporting & Monitoring of Data Protection

17.1 The college takes its responsibility around data protection very seriously. In order to monitor any data protection breaches or requests for information either by an individual or at an organisational level, the college will monitor requests

via its Freedom of Information Tracker or its Internal Personal Data Breach Register. This information is then feed into the college's management data dashboard. This dashboard will be monitored monthly in order to highlight any risks to the college or an individual. The data will also be used to highlight any additional training needs.

17.2 All actual or suspected personal data breaches must be reported immediately in accordance with the College Data Breach Notification Policy.

17.3 As well as being reviewed at management team meetings this information will also be monitored and appropriate committees and governance board.

18. Complaints and Appeals

18.1 The College will maintain a specific process for handling data protection complaints.

18.2 The College maintains a Data Protection Complaints Procedure. Complaints will be recorded, investigated, monitored and reported through a Data Protection Complaints Register.:

- be recorded in a Data Protection Complaints Register;
- be acknowledged within a reasonable timeframe;
- be investigated by an appropriately authorised member of staff;
- be responded to promptly;
- identify lessons learned and corrective actions;
- be retained in accordance with the Data Retention Policy.

18.3 Individuals dissatisfied with the outcome may complain to the Information Commissioner's Office (ICO).

18.4 Complaints will be acknowledged within 30 calendar days of receipt and investigated without undue delay.

Individuals may raise concerns with the Information Commissioner's Office (ICO) via www.ico.org.uk.

19. Conclusion

19.1 Compliance with UK GDPR is the responsibility of all members of the College. Any deliberate breach of the Data Protection Policy may lead to disciplinary action being taken, or access to College facilities being withdrawn, or even a criminal prosecution. The College will review and update this policy in line with organisational needs.

19.2 Any questions or concerns about the interpretation or operation of this policy should be taken up with the designated College Data Controller

Appendix 1

Access to Personal Information Request Form.

I, _____ (insert name) wish to have access to either (delete as appropriate)

1. All the data that the College currently has about me, either as part of an automated system or part of a relevant filing system; or
2. Data that the College has about me in the following categories:
 - **Academic marks or course work details.**
 - Academic or employment references.
 - Disciplinary records.
 - Health and medical matters.
 - Political, religious or trade union information.
 - Any statements of opinion about my abilities or performance.
 - Personal details including name, address, date of birth etc.
 - Other information: please list below.

(Please tick as appropriate)

Requests are normally free of charge. Fees may only be charged where permitted by applicable data protection legislation. The College will undertake reasonable and proportionate searches when responding to Subject Access Requests.

Name

Address

Date

Please return this form to the Data Protection Officer (Director of Finance). You may be asked to provide evidence of proof of identity before information is released to you and sign a receipt form to confirm receiving the information.