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 new General Data Protection Regulation.

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	6
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 Date	31 March 2023
Review Ratified/Approved Date	Operations Committee 14.06.2023
Next Review Due	March 2025

1. Introduction

1.1. Fircroft College as a data processer and data controller 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 General Data Protection Regulation (GDPR). In summary these state that personal data shall:

1.2. Processed lawfully, fairly and in a transparent manner in relation to individuals;

1.3. 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;

1.4. Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

1.5. 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;

1.6. 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 GDPR in order to safeguard the rights and freedoms of individuals;

1.7. 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;

1.8. Not be transferred to a country outside the European Economic Area, unless that country has equivalent levels of protection for personal data.

1.9. Article 5(2) of the General Data Protection Regulation requires that

1.10. "The controller shall be responsible for, and be able to demonstrate, compliance with the principles."

1.11. 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 staffs adhere to the GDPR principles at all times.

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, Head of Finance and Regulatory Compliance) 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 GDPR.

2.4 "Sensitive personal data" is information as to the subject's race or ethnic origin, political opinions, religious beliefs, trade union membership, physical or mental condition, sexual orientation and offences committed or alleged.

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 GDPR.

3. Individuals Rights Under GDPR

3.1.1. The College is dedicated to ensuring individuals rights under GDPR are upheld. Any information the College holds about an individual will be available under 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 the rights related to automated decision making allow an individual the right to obtain human intervention when automated processes have been used.

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

4. Responsibilities of Staff

4.1 Staff are responsible for

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

4.1.2 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.

4.2 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 General Data Protection Regulation.

5. Data Security

5.1 All members of staff are responsible for ensuring that:

5.1.1 Any personal data which they hold is kept securely.

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

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

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

5.2 Personal information should be:

5.2.1 Kept in a locked filing cabinet; or

5.2.2 in a locked drawer; or

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

6. Remote Access

6.1 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.

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

7. Student Obligations

7.1 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 Lee Goodway, Head of Student Experience). Any student who requires further clarification about this should contact the designated Student Data Controller.

8. Rights to Access Information

8.1 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.

8.2 The College will make no charge for the first occasion that access is requested, but may make a charge each subsequent request at its discretion.

9. Publication of Fircroft College Information

9.1 The General Data Protection Act and Freedom of Information Act 2000 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.

10. Sensitive Information Consent

10.1 In most cases, personal data can only be processed with consent of the individual. If the data is 'sensitive' data, express consent must be obtained. This could include, student support progress, previous criminal convictions. The college has a duty of care to all staff and students and must therefore make sure that all users and employees of the College do not pose a threat or danger to other users.

11. Processing Sensitive Information

11.1 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.

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

12.1 The College acts as the Data Controller and Data Processor under GDPR, and the Governing Body is therefore ultimately responsible for implementation. However, there are designated Data Controllers dealing with day to day matters. The first point of contact for enquirers is:

Stephen Hayden, Head of Finance and Regulatory Compliance, 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.

13. Use of CCTV.

13.1 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 Code of Practice. (Appendix 2)

14. Examination Marks

14.1 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.

15. Retention of Data

15.1 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.

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

16. Reporting & Monitoring of Data Protection

16.1 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 it's Freedom of Information Tracker or it's 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.

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

17. Complaints and Appeals

17.1 Any complaints or appeals received in respect of this policy will be dealt with under the College's Complaints Procedure. If applicants are dissatisfied with the outcome of the Complaints Procedure they may seek an independent review from the Information Commissioner. Requests for review by the Information Commissioner should be made in writing to:

The Information Commissioner
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF
Tel. 01625-545-700 Fax. 01625-545-510

18. Conclusion

18.1 Compliance with 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.

18.2 Any questions or concerns about the interpretation or operation of this policy should be taken up with the designated College Data Controller (Director of Student Services & Inclusion).

Appendices

1. Access to Personal Information request.
2. CCTV Code of Practice.

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)

I understand that I will have to pay a fee of _____
(Fee of £10 per request payable for second and subsequent requests for the same category (ies) of information within a twelve month period

Name

Address

Date

Please return this form to the Data Protection Officer (Head of Finance & Regulatory Compliance). 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.

Appendix 2
Closed Circuit Television (CCTV) – Code of Practice

1. Introduction

1.1. The purpose of this code is to regulate the management, operation and use of the CCTV system.

1.2. The CCTV system is owned by Fircroft College and follows General Data Protection Regulation (GDPR) guidelines. The Code of Practice is subject to reviews as and when required.

1.3. Currently there is only one camera which is used for 'live' surveillance by Reception. This camera covers the main entrance and is used as additional security so that visitors to the College can be identified. The use of this 'live' camera will be reviewed in line with the new reception build. There are other cameras located around the college which have the option to monitor 'live' surveillance but this is done at the college's discretion.

1.4. Any images recorded are only available to named staff and members of the Leadership Team who may be required to investigate any alleged incident.

2. Objectives of the Scheme

2.1. To protect staff, students, visitors and the property of the College.

3. Statement of Intent

3.1. The CCTV system will be registered with the Information Commissioner under the terms of the General Data Protection Regulation and will comply with the requirements of GDPR and the Commissioner's Code of Practice.

3.2. Cameras will only be used to capture any activity that has occurred and for the purpose of securing the safety of staff and users of the College.

3.3. Cameras will be used to safeguard the College students, staff, premises and assets.

3.4. Any recording secured as a result of the CCTV will not be used for any commercial purpose. Recordings will only be released to the emergency services in the investigation of a crime and with written authority of the police.

3.5. The planning and design of the system endeavours to ensure the safety and security of staff and students with maximum effectiveness and efficiency but it is not possible to guarantee that the system will cover or detect every single incident taking place in the area of coverage.

3.6. Warnings signs required by the Code of Practice of the Information Commissioner have been placed in and around the College.

4. Operation of the System

4.1. The scheme will be administered by the College's Head of Business Infrastructure or his/her deputy.

4.2. The CCTV system will operate 24 hours a day, 365 days of the year. A member of the IT team will check the system on a regular basis to make sure the system is working and recording properly.

4.3. Access to the system will be limited to the named officers and Leadership Team. Named officers must be present where the monitoring equipment is based. (See section 8.3)

4.4. Other administrative duties will include:

4.4.1. The monitoring of hard disc space

4.4.2. Recording details of serious incidents.

5. Storage and Disclosure procedure

5.1. In order to maintain the integrity of the media recovered by the system and the use in any future proceedings it is important that the following procedure is followed when extracting recordings.

5.1.1. Each item of media (CD or USB) must be identified by a unique mark.

5.1.2. Before using each item of media (CD/USB) it must be cleaned of any previous recordings.

5.1.3. The Head of Business Infrastructure must note the date and time and unique reference number in a register when copies of media files are made for the Police or authorised persons. Media files can only be released to the Police on the understanding that the media item is the property of the College and be treated in accordance with this code. The college has the right to refuse permission for the Police to pass to any other person or body the media item or any part of the information contained thereon.

5.1.4. If the media is to be archived a reference must be made in the Student Services register.

5.1.5. Archived media must be locked away in a safe and secure area.

5.1.6. Media can be viewed by the Police for prevention and detection of crime, and by the named officers for supervisory purposes, authorised demonstrations and training.

5.1.7. Viewing of media items by the Police or authorised body must be recorded in a log book.

5.1.8. If the Court requires the release of the original media item this will be produced from the secure evidence store, complete in its seal bag.

5.1.9. If a request is received from another body, e.g. solicitors, to view or release media items this will be referred to the Director of Student Services & Inclusion. They are required to see and record satisfactory documents of the request showing that they are required for legal proceedings, a subject access request or in response to a court order. A fee can be charged in such circumstances.

5.1.10. Retention of any media file will be kept secure and retained in line with the Data Protection 2018 Act.

6. Breaches of the CCTV Code

6.1. Any breaches of the Code of practice will be investigated by the appropriate Leadership Team member in order for him/her to assess if disciplinary action is appropriate.

7. Complaints

7.1. Any complaints about Fircroft College's CCTV system should be referred to the Head of Business Infrastructure to be dealt with under the complaints procedure or the Staff Grievance procedure as appropriate.

8. Request for Data

8.1. GDPR provides individuals the right to access any data held by the College. This also includes those obtained by CCTV.

8.2. Requests for data should be made on the appropriate request form and sent to the Head of Finance & Regulatory Compliance.

8.3. Officers of the College permitted to view CCTV recordings are:

- Leadership Team
- Head of Business Infrastructure /IT Network Coordinator
- Necessary Team Leaders
- Overnight Security
- Evening Supervisor