FIRCROFT COLLEGE OF ADULT EDUCATION

Data Protection Policy

1. Introduction

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 Protection Act 1998 (the 1998 Act). In summary these state that personal data shall:

- Be obtained and processed fairly and lawfully and shall not be processed unless it meets the conditions set out in this policy.
- Be obtained for a specified and lawful purpose and shall not be processed in any manner incompatible with that purpose.
- Be adequate, relevant and not excessive for those purposes.
- Be accurate and kept up to date.
- Be processed in accordance with the data subject's rights.
- Be kept safe from unauthorised access, accidental loss or destruction.
- Not be transferred to a country outside the European Economic Area, unless that country has equivalent levels of protection for personal data.

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 above principles at all times.

2. Status of the Policy

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.
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 (Alex Jarvis, Head of Staff and Student Support) initially. If the matter is not resolved it should be raised as a formal grievance.

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 the Act.

"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.

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 Data Protection principles.

3. Notification of Data Held and Processed

All staff, students and other users are entitled to:

- Know what information the College holds and processes about them and why.
- Know how to gain access to it.
- Know how to keep it up to date.
- Know what the College is doing to comply with its obligations under the 1998 Act.

4. Responsibilities of Staff

Staff are responsible for

- Checking that any information that they provide to the College in connection with their employment is accurate and up to date.
- Informing the College of any changes to information which they have provided. E.g. changes of address.
- Checking the information that the College will send out from time to time, giving details of information kept and processed about staff.
- 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.

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 Data protection Act 1998.

5. Data Security

All members of staff are responsible for ensuring that:

- Any personal data which they hold is kept securely.
- Personal information is not disclosed either orally, (including by telephone) or in writing or accidentally or otherwise, to any unauthorised third party.
- Personal information is not disclosed without the express authorisation of the Principal or Staff/Student Data Controller.

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

Personal information should be:

- Kept in a locked filing cabinet; or
- in a locked drawer; or
- If it is computerised, is password protected.

6. Remote Access

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. Student Obligations

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 registration 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 (Sue Guest, College Registrar). Any student who requires further clarification about this should contact the designated Student Data Controller.

8. Rights to Access Information

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. (Freedom of Information Policy) Please see the Head of Student and Staff Support for the "Access to Personal Information Form" (Appendix 1) form.
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

The Data Protection Act 1998 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

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

Sometimes it is necessary to process information about a person's health, criminal convictions, race and 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 the Designated Data Controller/s

The College is the Data Controller under the Act, 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:

Alex Jarvis, Head of Student & Staff Support, 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.

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

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

The College will keep some forms of information for longer than others. Because of storage problems, information about students cannot be kept indefinitely, unless there are specific requests to do so. The College Data Retention Schedule is attached. (Appendix 3)
After the retention date has been reached any confidential information will be disposed of in accordance with existing arrangements.

16. Associated Documents and Related Policies

Freedom of Information, Data Retention Schedule, Staff Disciplinary Procedure, Social Media Policy, Electronic and Telecommunication Policy, College Charter. The Secure Storage, Handling, Use, Retention and Disposal of Disclosure Information, (G Drive. Policies and Procedures)

17. Complaints and Appeals

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

Compliance with the 1998 Act 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.
Any questions or concerns about the interpretation or operation of this policy should be taken up with the designated College Data Controller. (Head of Staff and Student Support)

Appendices

1. Access to Personal Information request.
2. CCTV Code of Practice.
3. Retention of Data Schedule for Fircroft College.

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

Fircroft College

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

Introduction

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

The CCTV system is owned by Fircroft College and follows Data Protection Act guidelines. The Code of Practice is subject to reviews as and when required.

Only one camera 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. There are other cameras located around the college which are NOT used for 'live' surveillance.

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

Objectives of the Scheme

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

Statement of Intent

The CCTV system will be registered with the Information Commissioner under the terms of the Data Protection Act 1998 and will comply with the requirements of the Data Protection Act and Commissioner's Code of Practice.

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.

Cameras will be used to safeguard the College premises and assets.

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.

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.

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

Operation of the System.

The scheme will be administered by the College Deputy Principal or his/her deputy and Unison Security Company.

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

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

Other administrative duties will include:

- the maintaining of hard disc space
- recording details of serious incidents.

Storage and Disclosure procedure.

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.

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

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

3. The Deputy Principal 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.

4. If the media is to be archived a reference must be made in the Deputy Principal's register.

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

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.

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

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.

9. If a request is received from another body, e.g. solicitors, to view or release media items this will be referred to the Deputy Principal or designated person. 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.

Breaches of the Code.

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

Complaints.

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

Request for Data.

The Data protection Act provides individuals the right to access any data held by the College. This also includes those obtained by CCTV.

Requests for data should be made on the appropriate request form and sent to the Head of Staff and Student Support.

Officers of the College permitted to view CCTV recordings are:

Principal
Deputy Principal
Head of Staff and Student Support
Registrar
Finance Assistant.
Receptionist

Appendix 3.

Retention of Data Schedule for Fircroft College.

The table below lists the information that is currently recorded and kept by Fircroft College, along with its period of retention

Destruction of any records can only be authorised by a member of the senior management team and can only be by confidential shredding or through a secure third party.

Area	**Record**	**To be maintained by**	**Period of Retention**
HR	Staff Personal Files including Contracts of employment,	HSSS	Indefinitely
	Grievance/disciplinary hearings	HSSS	6 years from end of employment
	Health information	HSSS	6 years from end of employment
	Recruitment Files	HSSS	6 Months from date of the decision
	Sickness Absence Monitoring Records	HSSS	2 years
	Holiday records	HSSS	2 years
	CRB Disclosures	HSSS	Not kept
	Working Directive opt out	HSSS	6 years from end of employment
	Staff Professional Development Records and Files	HSSS	6 Years
	Staff Appraisal Information	HSSS	6 years
	Facts re redundancies	HSSS	3 years if < 20, 12 years if > 20
Finance	Published Financial Accounts	DPFR	Indefinitely
	Financial Records including invoices,	DPFR	3 or 6 Years – see

	receipts, ledgers and accounts – hard copy and electronic		Financial Procedures 6.1 for further information
	Payroll Data including pensions information	DPFR	6 Years following cessation of an individual's employment
	Pension calculations – employee and employer	DPFR	Indefinitely
	Payroll calculations	DPFR	6 years
	Non statutory deductions	DPFR	6 years
	SMP, SSP	DPFR	3 years
	Correspondence & returns to HMRC	DPFR	Indefinitely
	Tenders and Time-expired Contracts	DPFR	6 Years
	Internal and External Audit Reports	DPFR	6 Years
Finance	Employers Liability Certificate	DPFR	40 Years
	Insurance claims	DPFR	6 years after settlement
	All original documentation relating to grant funded projects	DADP/DPFR	In line with the requirements of the funding bodies
Area	**Record**	**To be maintained by**	**Period of Retention**
Governance	Minutes of the Board of Governors and its Standing Committees	The Clerk to the GB	Historical record – kept in perpetuity
	Agenda, papers and other records of the Board of Governors	The Clerk to the GB	10 Years – some historical documents kept in perpetuity for research purposes
Student Records	Student Records – electronic and hard copy	Registrar	10 Years (rather than 6 – agreed SG/FL)
	Attendance, Conduct, Examination and Assessment Records	Registrar	10 years (rather than 6 – agreed SG/FL)
Academic	Quality System Files	DADP	8 Years
Marketing	College Contacts Database	Marketing Officer	Database reviewed every 3 years
Student Support	Student Advice and Guidance Records	Head of Information, Advice & Guidance	5 Years following cessation of an individual's enrolment
	Learner Support Fund Records	DPFR	6 Years
	Childcare Records	Short Course Facilitator	3 Years following cessation of a child's placement in the Centre
Health & Safety/ Premises	Accident Register	Health & Safety Officer	6 Years
	Health and Safety Records – including risk assessment, audits, PAT testing etc.	DPFR	10 Years
	CCTV Recordings	DPFR	28 Days
Management	Line Management Files and Records	All Line Managers	Duration of individual's employment then forwarded to Personnel for disposal

IT/Legal Compliance	Software Licences and Hardware Registers	DPFR	5 Years
	Data Protection Registration	Head of Staff and Student Support	10 Years
	Copyright Clearance Records	Head of Staff and Student Support	2 years for teaching Materials. For the duration of usage of web based materials