Document No. PP
Issue No. 1
Issue Date: 2018-05-25
Renewal Date: 2019-05-25
Originator: Kate Frith
Responsibility: Director of Resources

FULLHURST
COMMUNITY COLLEGE
EST. 1991

GDPR Data Protection Policy

1. Introduction

In order to operate efficiently Fullhurst Community College has to collect and use information about people with whom it works and the students it provides an education to. These may include members of the public, current, past and prospective employees, clients and customers, students, parents and suppliers. In addition it may be required by law to collect and use information in order to comply with the requirements of central government.

The school is committed to ensuring personal data is properly managed and that it ensures compliance with current data protection legislation. The school will make every effort to meet its obligations under the legislation and will regularly review procedures to ensure that it is doing so.

You must read, understand and comply with this privacy standard when processing personal data on our behalf, and attend training on its requirements. Your compliance with this privacy standard is mandatory.

2. Scope

This policy applies to all employees, governors, contractors, agents and representatives, volunteers and temporary staff working for or on behalf of the school.

This policy applies to all personal data created or held by the school whether it relates to past or present employees, workers, students and/or other data subjects. This policy applies to personal data in whatever format (e.g. paper, electronic, email, microfiche, film) and however it is stored, (for example ICT system/database, shared drive filing structure, workbooks, email, filing cabinet, shelving and personal filing drawers).

Personal data is information about living, identifiable individuals, or an identifier or identifiers that can be used to identify a living individual. It covers both facts and opinions about the individual. Such data can be part of a computer record or manual record.

Current data protection legislation does not apply to access to information about deceased individuals. However, the duty of confidentiality may continue after death.

3. Responsibilities

Overall responsibility for ensuring that the school meets the statutory requirements of any data protection legislation lies with the Governors, and the Chair of Governors has overall responsibility for information management issues. They have delegated the day-to-day responsibility of implementation to the Principal.

The Principal is responsible for ensuring compliance with data protection legislation and this policy within the day-to-day activities of the school. The Principal is responsible for ensuring that appropriate training is provided for all staff.

All contractors who hold or collect personal data on behalf of the school by way of written contract are responsible for their own compliance with data protection legislation and must ensure that personal information is kept and processed in line with data protection legislation and only upon instruction from the school, via a contract.

4. The requirements

Data protection legislation stipulates that anyone processing personal data must comply with principles of good practice; these principles are legally enforceable. The six principles require that personal data:

- shall be processed fairly and lawfully and transparently;
- shall be obtained only for one or more specified and lawful purposes and shall not be further processed in any manner incompatible with that purpose or those purposes;
- shall be adequate, relevant and not excessive in relation to the purpose or purposes for which it is processed;
- shall be accurate and where necessary, kept up to date;
- shall not be kept in a form which permits identification of data subjects for longer than is necessary for that purpose or those purposes for which data is processed, and
- shall be kept secure i.e. protected by an appropriate degree of security.

In addition the data shall be processed in accordance with the rights of data subjects. (See Part 16.)

Personal data shall also not be transferred to a country unless that country or territory ensures an adequate level of data protection or another secure method of transfer is guaranteed.

5. Notification

The Digital Economy Act 2017 requires every data controller who is processing personal data, to notify and renew their notification, on an annual basis. Failure to do so is a criminal offence. The Information Commissioner maintains a public register of data controllers, in which the school must be registered.

The School will review the Data Protection Register - (https://ico.org.uk/esdwebpages/search) annually, prior to renewing its notification to the Information Commissioner.

6. Privacy notices

Whenever information is collected about individuals they must be made aware of the following at that initial point of collection:

- the identity of the data controller, e.g. the school;
- contact details of the Data Protection Officer;
- the purpose that the information is being collected for;
- any other purposes that it may be used for;
- what the lawful basis is for processing the data;
- who the information will or may be shared with;
- if the data is transferred outside of the EU, and if yes, how is it kept secure;
- how long the data will be kept for; and
- how data subjects can exercise their rights.

The school will review its privacy notices annually and alert students and parents to any updates.

7. Conditions for processing

Processing of personal information may only be carried out where one of the conditions of Article 6 of the GDPR has been satisfied. Some of the purposes for which the GDPR allows processing are set out below:

- the data subject has given his or her consent;
- the processing is necessary for the performance of a contract with the data subject;
- to meet our legal compliance obligations;
- to protect the data subject's vital interests; or
- to pursue our legitimate interests for purposes where they are not overridden because the processing prejudices the interests or fundamental rights and freedoms of data subjects. The purposes for which we process personal data for legitimate interests need to be set out in applicable privacy notices.

We will identify and document the legal ground being relied upon for each processing activity.

Processing of special category (sensitive) personal data may only be carried out if a condition in Article 9 of the GDPR is met as well as one in Article 6.

8. Data Protection Officer

The school shall appoint a Data Protection Officer (DPO) in line with the requirements of the GDPR. The DPO shall be responsible for overseeing this privacy standard.

Staff should contact the DPO with any questions about the operation of this privacy standard or the GDPR or if they have any concerns that this privacy standard is not being or has not been followed. In particular, staff must always contact the DPO in the following circumstances:

- if they are unsure of the lawful basis which is being relied on to process personal data (including the legitimate interests used by the school);
- if privacy notices need to be drafted;
- if there is any uncertainty about the retention period for the personal data being processed;
- if there is any uncertainty about what security or other measures need to be implemented to protect personal data;
- if there has been a personal data breach; or
- if any assistance is required in dealing with any rights invoked by a data subject.

9. Data protection impact assessments

The school shall undertake high risk Data Protection Impact Assessments in line with the requirements of the GDPR and as per the Information Commissioner's Office (ICO) guidance.

10. Data breaches

All employees, governors, contractors, agents and representatives, volunteers and temporary staff shall report any actual or suspected security incident or data breach immediately to senior management and the school's Data Protection Officer. Staff who report an actual or potential breach should not attempt to investigate the matter themselves, and should preserve all evidence relating to the breach.

The school shall report any personal data breach to the ICO in line with the requirements of the GDPR. In certain circumstances, (for example, where a data breach is likely to result in a high risk to the data subject's rights and freedoms) data controllers are also required to inform the data subject in the event of a breach.

11. Contracts

The school shall ensure that a legally binding contract is in place with all of its data processors in line with the requirements of the GDPR.

12. Consent

Where the school processes data with consent (for example, to publish photographs of children, to send direct marketing emails about school uniform for sale) it will ensure that the consent is freely given, specific, informed and unambiguous**,** and the consent is recorded.

Usually the school will rely on another legal basis for processing (and will not require explicit consent), to process most types of special categories of personal data.

The school will keep records of all consents so that the School can demonstrate compliance with consent requirements. Data subjects can withdraw their consent to processing at any time.

13. Information society services

Where the school offers information society services (online services with a commercial element) targeted at children, it will take reasonable steps to seek the consent of the child's parent or guardian if the child is under 13 years of age.

14. Direct marketing

Where the school sends any direct marketing (the promotion of aims and ideals as well as selling goods and services) via electronic communications e.g. email, SMS text, fax or recorded telephone messages, it will only do so if the recipient has given explicit consent to receive them e.g. has ticked a box to 'opt in'.

15. Provision of data

It is a criminal offence to knowingly or recklessly obtain or disclose information about an individual without legitimate cause. Relevant, confidential data should only be given to:

- other members of staff on a need to know basis;
- relevant Parents/Guardians;
- other authorities if it is necessary in the public interest, e.g. prevention of crime, safeguarding; or
- other authorities, such as the Local Authority and schools to which a student may move, where there are legitimate requirements (DfEE leaflet 0015/2000 entitled "Student Records and Reports" issued in March 2000 covers data protection issues and how and what information should be transferred to other schools. DfES/0268/2002 provides further information).

The school should not disclose anything on a student's record which would be likely to cause serious harm to their physical or mental health or that of anyone else. Therefore, those who create such records should ensure that such information is separated from other records.

Any disclosure of information to third parties should be in compliance with our privacy notice. In some circumstances, the data subject's consent may need to be obtained.

Where there is doubt, or statutory requirements conflict, you should consult the DPO, who may consider that legal advice should be obtained. Where there are safeguarding concerns, the matter should be referred to the school's Designated Safeguarding Lead (DSL).

When giving information to an individual, particularly by telephone, it is most important that the individual's identity is verified. If in doubt, questions should be asked of the

individual, to which only he/she is likely to know the answers. Information should not be provided to other parties, even if related. For example: in the case of divorced parents it is important that information regarding one party is not given to the other party to which he/she is not entitled. Care must always be taken when there is any doubt about parental responsibility.

16. The individual's rights

Any person whose details are held by the school is entitled to ask for a copy of information held about them (or child for which they are responsible). They are entitled to see if the data held are accurate, and who it is shared with.

When a request is received it must be dealt with promptly; a response must be provided as soon as possible and within one month and in some instances, for education records, 15 school days. All staff must recognise and log such a request with the Data Protection Officer.

The school cannot charge for responding to a subject access request unless the request is repeated manifestly unfounded or excessive. The school can charge up to £50 (on a sliding scale for photocopying charges) for access to a student's educational record.

When providing the information the school must also provide a description of why the information is processed, details of anyone it may be disclosed to and the source of the data.

Staff of the school must also recognise and log the following requests with the Data Protection Officer, and all must be answered within one month:

- right to rectification of inaccurate data;
- right to erasure of personal data if it is no longer necessary;
- right to restriction of processing in specific circumstances;
- right to portability of data to a third party;
- right to challenge processing which has been justified on the basis of the school's legitimate interests or in the public interest;
- right to prevent processing that is likely to cause damage or distress;
- right to object to decisions based on automated processing; and
- right to complain to the supervisory authority.

Data subjects also have the right to receive certain information about the school's processing activities.

17. Provision of data to children

In relation to the capacity of a child to make a subject access request, guidance provided by the Information Commissioner's Office has been that by the age of 12 a child can be expected to have sufficient maturity to understand the nature of the request. A child may of course reach sufficient maturity earlier; each child should be judged on a case by case basis.

If the child does not understand the nature of the request, someone with parental responsibility for the child, or a guardian, is entitled to make the request on behalf of the child and receive a response.

Students who submit requests to access their educational records should be allowed to do so unless it is obvious that they do not understand what they are asking for.

18. Parents' rights

An adult with parental responsibility can access the information about their child, as long as the child is not considered to be sufficiently mature. They must be able to prove their parental responsibility and the school is entitled to request relevant documentation to evidence this as well as the identity of the requestor and child. The school has the right to ask the child if they object to release of information to the parent if the child is deemed mature enough to make such a decision.

In addition, parents have their own independent right under The Education (Pupil Information) (England) Regulations 2000 of access to the official education records of their children. Students do not have a right to prevent their parents from obtaining a copy of their school records (as defined in the Education Act).

19. Information security

Personal data must be secured by appropriate technical and organisational measures against unauthorised or unlawful processing, and against accidental loss, destruction or damage. The school will develop, implement and maintain such safeguards as are appropriate to our size, scope and available resources. All members of staff are responsible for protecting the personal data that the school holds, and must follow all procedures and technologies that we put in place to maintain the security of personal data.

All members of staff should be constantly aware of the possibility of personal data being seen by unauthorised personnel. For example, possibilities may arise when computer screens are visible to the general public; files may be seen by the cleaners if left on desks overnight (all papers must be locked in cabinets when not in use).

The use of computer passwords is a requirement of the school to avoid unauthorised access. All removable devices e.g. laptops, USB sticks, personal mobile phones and digital cameras must not be used to store school data unless they comply with the school Online Safety Policy and Staff Acceptable Use Policy.

All members of staff should take care when transporting paper files between sites. No personal data is ever to be left unattended off site e.g. in a car overnight, on view to family members when working at home.

Staff should not email personal or sensitive data to users outside of the school but use AnyComms Plus or ask the SIMS manager, Paul Barton, to send the data via encrypted Word documents.

20. Maintenance of up to date data

Out of date information should be discarded if no longer relevant. Information should only be kept in an identifiable form as long as needed, for legal or business purposes. The school will take all reasonable steps to destroy or erase from its systems all personal data that it no longer requires.

In reality most relevant information should be kept for the period during which the person is associated with the school plus an additional period which the school has determined. Under GDPR the school must produce a Retention and Disposal Policy to clarify this. All members of staff must comply with the school's policies and procedures in relation to data retention.

21. Inaccurate data

Personal data must be accurate and, where necessary, kept up to date. If an individual complains that the personal data held about them is wrong, incomplete or inaccurate, the position should be investigated thoroughly including checking with the source of the information. This must be answered within one month. In the meantime a caution should be marked on the person's file that there is a question mark over the accuracy. An individual is entitled to apply to the court for a correcting order and it is obviously preferable to avoid legal proceedings by working with the person to correct the data or allay their concerns.

22. Recording of data

Records containing personal data should be kept in such a way that the individual concerned can inspect them. It should also be borne in mind that at some time in the future the data may be inspected by the courts or some legal official. It should therefore be correct, unbiased, unambiguous, factual and clearly decipherable/readable. Where information is obtained from an outside source, details of the source and date obtained should be recorded.

Any person whose details, or child's details, are to be included on the school's website will be required to give written consent unless it is a legal requirement (e.g. Governors' details). At the time the information is included all such individuals will be properly informed about the consequences of their data being disseminated worldwide.

The school will keep records of all of its data processing activities.

23. Photographs

Whether or not a photograph comes under the data protection legislation is a matter of interpretation and quality of the photograph. However, the school takes the matter extremely seriously and seeks to obtain parents'/students' permission for the use of photographs outside the school and, in particular, to record their wishes if they do not want photographs to be taken of their children.

24. Breach of the policy

Non-compliance with the requirements of data protection legislation by the members of staff could lead to serious action being taken by third parties against the school. Non-compliance by a member of staff is therefore considered a disciplinary matter which, depending on the circumstances, could lead to dismissal. It should be noted that an individual can commit a criminal offence under the law, for example, by obtaining and/or disclosing personal data for his/her own purposes without the consent of the data controller.

25. Further information

Further advice and information about data protection legislation, including full details of exemptions, is available from the ICO website at www.ico.org.uk, or from Leicester City Council's Information Governance & Risk Team. Email info.requests@leicester.gov.uk

26. Review of the policy

This policy is to be reviewed bi-annually. We reserve the right to change this privacy standard at any time.

27. Glossary

Data controller	A data controller is the individual or the legal person who controls and is responsible for the keeping and use of personal information on computer or in structured manual files. The school is the data controller for all personal data relating to company personnel (including past or prospective company personnel) and for personal data relating to students or others which is collected in the course of the school's work.
Data subject	The individual who the data or information is about
Educational record	The educational record is confined to information that comes from a teacher or other employee of a local authority or school, the student or their parents. Communications about a particular child from principals and teachers at a school and other employees at an education authority will therefore form part of that child's official educational record, as will correspondence from an educational psychologist engaged by the governing body under a contract of services. It may also include information from the child and their parents, such as information about the health of the child. Information kept by a teacher solely for their own use does not form part of the official educational record.
Information Commissioner	The independent regulator who has responsibility to see that the data protection legislation is complied with. They can give advice on data protection issues and can enforce measures against individuals or organisations who do not comply with the law.
Notified purposes	The purposes for which the school is entitled to process that data under its notification with the Office of the Information Commissioner.

Personal data	Defined as 'data which relates to a living individual who can be identified from that data, or from that data and other information which is in the possession of, or is likely to come into the possession of, the data controller' or an identifier (the school is a data controller), and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other in respect of the individual.
Processing	Covers a broad range of activities such that virtually any use of personal information or data will amount to processing. Just holding or storing the data constitutes processing, as does organising, transferring, amending erasing or destroying them
Processed fairly and lawfully	Data must be processed in accordance with the provisions of data protection legislation. These include the data protection principles, the rights of the individual and notification.
Special category (sensitive) data	Information about racial or ethnic origin, sexual life, sexual orientation, religious beliefs (or similar), physical or mental health conditions, membership of a trade union, political opinions or beliefs, or biometric or genetic data.
Subject access request	An individual's request for personal data under the General Data Protection Regulation.