Data Protection Policy, Incorporating the Freedom of Information Schedule & the College Records Management Policy

Reviewed by: Owen Perkins
Ratified by: Full Governing Body
Next review: June 2021

Signed..... Richard Karn, Chair of Governors

Heathfield Community College Data Protection Policy, Incorporating the Freedom of Information Schedule & The College Records Management Policy

Summary

Our Data Protection Policy has been written by the college, benchmarked against identified best practice and government guidance on the legislation as it impacts on educational institutions. What follows in this document should be read in conjunction with other college policies on:

- Online Safety
- Anti-Bullying
- Behaviour
- Communication
- Copyright
- Discrimination
- The Freedom of Information schedule (which is found in **Appendix 1**)
- Records Management Policy (which is found in **Appendix 7**)

General Aims

The purpose of this document is to present guidelines for the safe and secure processing and use of personal data held within Heathfield Community College, including that data for which we have a legal obligation to make available under the Freedom of Information Act. It is also to ensure that personal information is dealt with correctly and securely and in accordance with Data Protection and other related legislation. It applies to information held and processed by the school regardless of the way it is collected, used, recorded, stored and destroyed, and irrespective of whether it is held in paper files or electronically.

Heathfield Community College will apply policies and procedures that are compliant with the East Sussex County Council (ESCC) Information Security and Data Protection Policies. It will also apply these policies in light of how the law affects educational institutions.

It is not possible to set out precautions and actions to cope with all circumstances and conditions, therefore anyone handling sensitive and confidential information MUST take responsibility and make considered judgements in terms of how they handle this information whilst delivering their service. If in any doubt they should seek clarification from their line manager and / or the Data Protection Officer / Data Protection Lead. This document will be reviewed and updated at least every two years by the Senior Leadership Team. Details of rights to access information and how we action a subject access request can be found in Appendix 3.

All staff involved with the collection, processing and disclosure of personal data will be aware of their duties and responsibilities and are required to comply with this policy.

What is Data Protection?

As a result of the interactivity of new technologies and the ease of communicating data, storing personal data electronically can potentially compromise personal security and that of others. Unless there is another legal basis for doing so, it is illegal to share the personal information held about an individual without that individual's permission, even

if it is not held electronically. Data Protection refers to the ways in which the college complies with the law about this. It is also about how we attempt to reduce the potential risks of storing personal data and how we go about making an individual's personal data available to them if they so wish.

Who has obligations as a result of this policy?

The requirements of this policy are mandatory for all staff employed by the school and any third party contracted to provide services within the school.

What is Personal Data?

Personal information or data is defined as data which relates to a living individual who can be identified, either directly or indirectly, from that data, or other information held. This includes IP addresses used by individuals to access College services. Information is the product of a collection of data, which can be held in many forms. For the purpose of this policy personal data and personal information are the same thing.

What is Confidential Data?

- personal information about pupils, staff and others
- School business records that are organisationally or publicly sensitive information
- sensitive business information, including commercially sensitive information about the College, East Sussex County Council, other agencies and contractors relating to commercial proposals or current negotiations
- Politically sensitive information
- Information relating to security, investigations and proceedings
- Any information which, if released, could cause problems or damage to individuals, the public, the school or another organisation. This could be personal, financial, reputation or legal damage

What are "Special Categories of Personal Data"?

- This is defined as: personal data consisting of information relating to the data subject with regard to racial or ethnic origin; political opinions; religious beliefs or other beliefs of a similar or philosophical nature; trade union membership; physical or mental health or condition; sexual life; the commission or alleged commission by the data subject of any offence; proceedings for any offence committed or alleged to have been committed by the data subject, the disposal of such proceedings or the sentence of any court in such proceedings.
- It also includes: genetic & biometric data that uniquely identifies an individual.
- We will only ask for these types of data to be processed if it is legal to do so. The legal bases for doing so are the following: consent; employment obligations; vital interests; it is in the public domain anyway; legal claims; substantial public interest; public health / social care; archiving
- We will only share these types of data if it is legal to do so, complies with the 6 data governance principles (see p5) and complies with data protection legislation for the following reasons: consent has to be explicitly given where it is needed; contracts with the data subject require us to do so; legal obligations require us to do so; vital interests make it necessary; public interest or official authority allows us to do so; legitimate interests exist, allowing us to do so.

What is a Data Controller?

"Data controller" means a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be processed

What is a Data Processor?

"Data processor", in relation to personal data, means any person (other than an employee of the data controller) who processes the data on behalf of the data controller.

What is a Privacy Impact Assessment?

A privacy impact assessment is a process which assists organizations in identifying and minimizing the privacy risks of new projects or policies. It should include: a question that asks "does the initiative or idea involve personal data &/or special category data?" If the answer to that is "yes", then it should ask what measures are in place to ensure that data is protected and is retained for only as long as it is necessary.

What is a Data Incident Management Plan?

A data incident management plan is a document that states what an organisation will do if there is a breach of data security.

The Legal Framework

The General Data Protection Regulations (GDPR) 2018. These are EU regulations governing the use and storage of data. Whilst the UK remains in the EU, they require data to be stored in specific ways and update the law in line with changes in technology since the last UK act of parliament. It also requires explicit consent to be given for all use of personal data and gives individuals the right to hold data controllers accountable for the uses that individual data can be put to. For example, Data Processors, as well as Data Controllers, can be held personally liable for data breaches.

Data Protection Acts 1998 and 2018. The 2018 act updates the 1998 Act to reflect the GDPR changes made by the EU in 2018. It requires anyone who handles personal information to notify the Information Commissioner's Office (ICO) of the type of processing it administers and to register with the ICO. Such organisations must comply with the data protection principles outlined in the GDPR. The Act grants to individuals rights of access to their personal data, compensation and prevention of processing.

The Human Rights Act 1998. Article 8 of the Human Rights Act gives everyone the right to respect for their private and family life, their home and their correspondence. The right to private life includes the right to have personal information, such as official records, photographs, letters, diaries and medical information kept private and confidential.

Common law duty of confidence. The common law duty of confidence requires that confidential information can be disclosed only with the permission of the person who

provided it, or the person the information relates to, unless there is an overriding public interest in disclosing the information without permission.

Computer Misuse Act 1990. The Computer Misuse Act details certain illegal activities, including: knowingly using another person's username or password without proper authority impersonating another person using email, online chat, web or other services misusing authorised access using, or helping another person to use, someone else's system for criminal activities modifying software or files so as to interfere with the system's operation or to prevent access to or destroy data deliberately introducing viruses, worms or other malware to cause a system malfunction.

Copyright, Designs and Patents Act 1988 The Copyright, Designs and Patents Act gives the creators of material control over how it is used, whether the material is on paper, film, CD, DVD, websites or databases.

Education and Inspections Act 2006 Sections 90 and 91 of the Education and Inspections Act provide statutory powers to Colleges for disciplining pupils for inappropriate behaviour or for not following instructions, both on and off College premises. Section 94 provides a defence for confiscation of inappropriate items from pupils as a disciplinary penalty.

The Freedom of Information Act 2000 Creates a public "right of access" to information held by public authorities.

Protection of Freedoms Act 2012 (sections 26 to 28) Creates a duty for schools using biometric systems, for automated payments systems, to notify each parents of a child about the use of the systems and to obtain the written consent of at least one parent before doing so.

Mental Capacity Act 2005 defines mental capacity, a phrase which creates limited exemptions to the need to seek consent.

Health & Safety at Work Act 1974 because GDPRs make health data "special category data", this law also becomes relevant

Heathfield Community College's Approach

Personal data will be recorded, processed, transferred and made available according to the GDPR (2018) and the Data Protection Act 2018 so that all data, from which people can be identified, will be protected. The six principles of data protection that Heathfield Community College subscribes to are that personal data must be:

1. Processed fairly, transparently and lawfully
2. Processed for specified limited purposes
3. Adequate, relevant and not excessive so that data used is minimised
4. Relevant, accurate and up-to-date
5. Held no longer than is necessary and securely destroyed
6. Confidential and with secure data integrity.

These 6 principles are as prescribed by the Information Commissioner's Office[1]. In addition to these 6 principles we will comply with the provisions of the Protection of Freedoms Act 2012 (sections 26 to 28), to notify each parent of a child and obtain the written consent of at least one parent before being able to use a child's biometric information for any automated system. (See exemptions to this and the procedure to be followed in the case of Looked After Children in **Appendix 4**, see **Appendix 5** for further information about biometric data.)

Registration

Heathfield Community College, as a data controller, has to register with the ICO and maintain a record of the information it holds and the purposes for which it obtains and uses personal data (including disclosure in any form to third parties). These details must be kept up to date and available for inspection by the Information Commissioner's Office.

Our data processing activities will be registered with the Information Commissioner's Office (ICO) as required of a recognised Data Controller. Details are available from the ICO: https://ico.org.uk/about-the-ico/what-we-do/register-of-data-controllers/

Further background that relates to the information contained within this policy can also be obtained from the ICO: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/

The Role of The Information Commissioner

The Information Commissioner is the body that oversees compliance with Data Protection legislation, and has powers to force organisations to process personal data lawfully.

Where a data subject is unhappy with some aspect of the processing of their personal information they have the right to complain to the Information Commissioner.

It is recommended that any such issue should be resolved locally between the school and the individual concerned where possible. Any enquiries subsequently received from the Information Commissioner will be referred to the College's Data Protection Officer.

Policy Statement

Heathfield Community College is committed to ensuring that all information is collected, processed, maintained and disclosed in accordance with the principles that personal data will be:

- processed lawfully, fairly and in a transparent manner
- collected and used for specified, explicit and legitimate purposes and not further processed in an incompatible way ('purpose limitation')
- adequate, relevant and limited to what is necessary for the purpose for processing ('data minimisation')
- accurate and where required, rectified without delay ('accuracy')
- not be kept in an identifiable form for longer than necessary ('storage limitation') i.e. in line with the school's retention schedule

[1] https://ico.org.uk/for-organisations/guide-to-data-protection/data-protection-principles/

- information must be appropriately secured/protected against unauthorised or unlawful processing, accidental loss, destruction or damage using appropriate technical or organisational measures ('integrity and confidentiality'). This includes:
  – using appropriate means of transmitting data
  – secure storage / disposal of personal information
  – where processing is sub-contracted or outsourced (e.g. payroll, disposal of confidential waste paper) there must be suitable Data Protection clauses in the contract

Personal information must also:

- be processed in accordance with the rights of data subjects e.g. right of access, right of erasure, rectification, restriction, portability and the right to object to certain processing (see section 12)
- not be transferred to countries outside the UK without adequate protections having been put in place eg that the people receiving the data are GDPR compliant or are registered with the EU-USA data security shield or have equivalent high level of data management protection.

General Statement

Heathfield Community College is committed to maintaining the above principles at all times. Therefore, the College will:

- Inform individuals why the information is being collected
- Inform individuals when their information is shared, and why and with whom it was shared
- Check the quality and the accuracy of the information it holds
- Ensure that information is not retained for longer than is necessary
- Ensure that when obsolete information is destroyed that it is done so appropriately and securely
- Ensure that clear and robust safeguards are in place to protect personal information from loss, theft and unauthorised disclosure, irrespective of the format in which it is recorded
- Share information with others only when it is legally appropriate to do so
- Set out procedures to ensure compliance with the duty to respond to requests for access to personal information, known as Subject Access Requests
- Ensure our staff are aware of and understand our policies and procedures

Responsibilities

All employees, Governors and any other individual handling personal information on behalf of the school have a responsibility to ensure that they comply with Data Protection legislation and the school's policies. In particular:

The **Headteacher** will:

- Ensure that the College has a named Data Protection Officer (DPO) / Data Protection lead (DPL) if the DPO is external, who has been chosen for their "requisite professional qualities", expert knowledge of data protection law & practices AND is adequately trained in the responsibilities of their role

- Ensure that the DPO / DPL does not have a conflict of interest as a data controller or data processor
- Ensure that the DPO has sufficient resources available to ensure that's their duties can be carried out effectively and without fear of prejudice
- Ensure that appropriate arrangements are in place to protect other people's personal and confidential data, either electronically or in hard copy.
- Ensure that the College's chosen Management Information System (MIS) is compliant with the most recent data protection legislation.
- Ensure that we only collect and process data, including "special categories" of data, if it is legal to do so and is consistent with the 6 principles of data governance (see p5)
- Ensure that personal data that is shared with the Local Authority / DfE and the College's technology providers is done only: to meet out statutory commitments; that it meets the requirements of the Data Protection Act and the General Data Protection Regulations; to be the minimum necessary to facilitate the efficient running of the College; and is shared and stored in a secure way
- Ensure that all external data processors, including those that use biometric data, have a data incident management plan as a part of their contractual arrangements with the College
- Ensure that all external data processors, including those that use biometric data, have a contractual agreement with the college about indemnifying the college for any loss incurred, financial or otherwise, by the college that results from a data breach for which the data processor is responsible
- Ensure that any company contracted to provide biometric automated systems uses systems that only allow biometric data to be obtained, used and stored in accordance with that Data Protection Act, including having a data incident management plan as a part of their contractual arrangements with the College
- Ensure that biometric data is NOT taken if one parent gives consent to the use of a child's biometric data AND another parent has objected in writing to that use.
- Ensure that parents are informed that in order to withdraw their consent for the use of biometric data, after having initially given consent, they must put this in writing to the college
- Ensure that biometric data is NOT taken if the child (whether verbally or non-verbally) objects or refuses to participate in the processing of their biometric data
- Ensure that the college provides reasonable alternative means of accessing services for those pupils who will not be using an automated biometric recognition system.
- Ensure all staff members and governors with access to pupils' personal information have enhanced Disclosure and Barring Service (DBS) clearance.
- Ensure employment contracts state that misuse of confidential information and information and communication technology (ICT) is a disciplinary matter.
- Ensure confidential information is accessible only to people who have a legitimate need to know it.
- Require staff and governors to use strong passwords to access electronically held confidential information and for those passwords to be changed at 90 day intervals
- Ensure that appropriate communication is in place to inform all visitors to the college site (including parents, pupils, staff and contractors) that CCTV is in operation on the premises and that this is used to ensure the safety and security of the buildings and the college community
- Ensure that all staff are aware of Data Protection policies and the legal requirements that affect them, including adequate training where appropriate

- Ensure that all staff and governors are aware that information containing personal data or that is private or confidential cannot be sent by email external to the college network unless from an address on the local authority secure email system to an address on the same system
- Ensure that all staff and governors are aware that if they carry confidential information out of College premises on College owned portable media (eg laptops, iPads, memory sticks), the media used to do this MUST be password / PIN protected AND have hard drive encryption in order to be allowed to connect to the college network.
- Staff or governors using their own devices will only be allowed to connect to the college network whilst on site using remote access AND if they have signed an agreement to recognise their understanding of the importance of maintaining strong PIN / password protection.[2]
- Ensure that all staff and governors are aware that personal data cannot be sent by email and NEVER in an attachment to an email UNLESS using the ESCC secure email system. Emails containing student / staff names are allowed for the efficient running of the College. When off site, College email should only be accessed using the remote access system OR webmail OR from an app that DOES NOT also access private email addresses.[3]
- Ensure that staff and governors, who have used their own portable media or other devices, whether their own or college owned, to fulfil their duties, will be asked to sign a leaving statement that they have deleted any private or confidential information from those devices BEFORE they leave.
- Ensure that a procedure is in place to remind all staff leaving employment of the college AND governors completing their term of office to return all College information, equipment, computer, portable media devices and software.
- Ensure that a procedure is place to remind all staff leaving employment and governors completing their term of office, who have used their own portable media or devices to fulfil their duties, who wish to dispose of, sell or return on guarantee that device, are reminded to delete any private or confidential information from their device BEFORE doing so.
- Require that, whilst off site, the College remote access system can only be accessed using 2 factor identification eg a card reader.
- Ensure that procedures are in place to store and dispose of confidential records securely. For example, the adopted Retention and Disposal Schedules (See **Appendix 8**), for the specific information and records being disposed, MUST be followed AND methods such as: cross-cut shredding; or pulping; or using the confidential waste bins where available; and keeping the waste in a secure place until it can be collected for secure disposal; and to NEVER put sensitive and confidential waste in normal waste bins.
- Ensure that procedures are in place to manage SIMS security access rights so that only the senior data / SIMS manager can have access to the SIMS process for downloading an individual's electronically held data records
- Ensure that procedures are in place to manage SIMS security access rights so that data access rights reflect those needed to fulfil each individual's job role
- Ensure that staff and governors receive adequate training to handle confidential information and ICT responsibly and securely

[2] Ditto

[3] This is a trial policy for the academic year 2018-19 that will be reviewed by the end of that year

- Make appropriate arrangements to inform all parents and carers that we hold personal information about each pupil and explain how we intend to use this information in the form of a privacy notice
- Make alternative arrangements to inform all parents and carers, who are without a broadband internet connection, about the content of the appropriate privacy notice
- Make appropriate arrangements to ensure that every student and member of staff is asked to give their consent for their image to be published electronically on the college website.
- Remind staff of the importance of carefully and sensitively selecting images for publication on the College Website and in not allowing such images to clearly identify individual students.
- Regularly remind staff that they need to check whether or not the parents / carers have declined to give consent for the image of their child to be used on the college website, before doing so. This is usually collected in advance on joining the school via the Internet and Network User's Agreement.
- Ensure that the educational trips policy includes a requirement for all trips, that require the transfer of personal data, especially international trips, to include adequate data protection planning before the trip can go ahead.
- Ensure that the educational trips policy includes provision for the safe transport of personal data by the trip leader whilst on the trip. This includes signing the data out at the beginning of the trip, signing it in at the end of the trip and lockable storage for the duration of the trip

The **Data Protection Officer / Internal Data Protection Lead** will:

- Be the first point of contact for the College with ICO & to ensure that the College cooperates with the ICO on all of its requests
- Ensure that the college has a process for ensuring that it is registered with the Information Commissioner's Office (ICO) on an annual basis.
- Ensure that the college has a process for, when there are changes to the type of data processing activities being undertaken by the college, notifying this to the ICO so that these details are amended in the ICOs register.
- Ensure that the college has a process for monitoring compliance with the GDPR & other data protection laws, as they change over time, as they affect schools in England
- Inform & advise the College leadership on appropriate training for all staff & governors about their obligations to comply with the GDPR & other data protection laws
- Ensure that the college has a process for guaranteeing that "Privacy Impact Assessments" are completed for all new data processing activities AND for all data processing activities that existed before GDPR became law
- Ensure that the college has a process for ensuring that "special categories" of data are not being processed by third party software providers unless absolutely necessary to the purpose of the data processing
- Ensure that the college has a process for complying with the provisions of the Protection of Freedoms Act 2012 (sections 26 to 28): to notify each parent of a child and obtain the written consent of at least one parent before being able to use a child's biometric information for any automated system. (See exemptions to this and the procedure to be followed in the case of Looked After Children in Appendix 4)

- Ensure that the college has an appropriate notification procedure in place should there be an information security incident / data breach, including a system in place to log and monitor all information security incidents, allowing for any trends to be picked up and for preventative measures to be put in place. Also to test that this procedure works.
- Ensure that breaches of personal, confidential or special categories of personal data shall be notified immediately to the individual(s) concerned, the Head Teacher and the ICO at the very latest within 72 hours (including weekends) of the breach.
- Ensure that the college has effective arrangements for every member of staff, parent or carer of every pupil and pupils, over the minimum age, governors, alumni, volunteers, job applicants and College customers to be sent a Privacy Notice (see Appendix 6). There should also be privacy notices for governors, lettings and other customers and for parents in terms of the data that we hold about the parents themselves. This may be made up of separate notices for separate uses of data AND it may also include "Just In Time" privacy notices for new uses of data as they arise. The notice should include a clear statement of the legal grounds for processing data. The notice will then be renewed in the autumn term of every College year and will be made available on the policies homepage of the College website.
- Ensure that the college has a process to allow pupils and parents to see the information that is held about their "educational record" within 15 days of a specific request being made to see the "educational record".
- Ensure that the college has a process to allow pupils to see the information that is held about them outside of their educational record within ONE calendar month of a request being made, unless providing that information is likely to satisfy one of the conditions for withholding information, for example, the likelihood of it resulting to harm to the child or another person as a result of providing that information.
- Ensure that the college has a process to allow parents, carers, legal guardians, staff and governors to see the information that is held about them within ONE calendar month of a request being made.
- Ensure that the college has a process to keep accurate and effective records of: sources of best practice advice used in the College, who the data controllers / joint controllers are, data protection audits, data maps, consent for data processing (where consent is needed), information security incidents, data breaches as they evolve over time, monitoring or processes, staff training, quality assurance processes, any external certification, the data protection budget and changes to data protection guidance as it evolves.
- Ensure that the educational visits officer / trip leaders are supported in the planning of all trips, that require the transfer of personal data, especially international trips, so that there is adequate data protection planning before the trip can go ahead.
- Ensure that the college has a process to follow an agreed data retention schedule and for all data to be securely deleted when it is no longer needed, when the retention period has expired and that ALL "special categories" of data are securely deleted before an appropriately short period after the pupil is no longer on roll. (See the data retention schedule in Appendix 8.)

All **staff** and **governors** that access other people's personal data will:

- Report any information security incident / data breach to the Data Protection Lead immediately as the College MUST inform the ICO within 72 hours of a major breach.

- Ensure that they are careful in using other people's confidential data so that students, and adults, other than appropriate College & LA staff, do not have access to other people's personal data, either electronically or in hard copy.
- NOT take personal or confidential information off the College premises on portable media eg laptops, iPads, memory sticks etc…) UNLESS it has been password / PIN protected AND encrypted.
- NEVER send personal data by email and NEVER in an attachment to an email UNLESS using the ESCC secure email system. Emails containing student / staff names are allowed for the efficient running of the College.
- When off site, College email should only be accessed using the remote access system OR webmail OR from an app that DOES NOT also access private email addresses.[4]
- NEVER access College emails on a home PC or other home owned device via an installed app such as e.g. Outlook or Mail on Apple products
- If they have used their own portable media to fulfil their duties, and who wish to dispose of, sell or return on guarantee that device, delete any private or confidential information from their device BEFORE doing so.
- On leaving college employment, if they have used portable media, whether their own or college owned, to fulfil their duties, delete any private or confidential information from those devices BEFORE they leave.
- Ensure that they comply with the College Policies on E-safety in regard of password sharing, password security and the regularity with which passwords should be changed.
- NOT allow pupils or other unauthorised people to access confidential paper or electronic records they do not have a right to see
- NOT disclose confidential information they have access to as part of their work to colleagues, friends or acquaintances who do not have a need to know
- NOT discuss information you have access to as part of your work on any social networking site or any unauthorised website
- NOT look up any information relating to your own family, friends or acquaintances unless you are authorised to do so.
- When selecting images for publication that include staff or students, will sensitively and carefully select them, and will ensure that the images chosen DO NOT enable individual students to be identified from an image or an image combined with accompanying text.
- Not use students' full names anywhere on the College website where the student can be identified in association with photographs.
- Check whether or not written permission from parents / carers and staff has been obtained before images of students / staff are electronically published.
- Seek the permission of the pupil and parents before their work is electronically published.
- Comply with LEA guidance on the adoption and use of biometric data, if the college chooses to adopt a new technology that use such data.
- Ensure that when planning a trip, that requires the transfer of personal data, especially international trips, there is adequate data protection planning before the trip goes ahead.
- Ensure that they follow the guidance on handling educational trips for the safe transport of personal data whilst on the trip. This includes signing the data out at

[4] This is a trial policy for the academic year 2018-19 that will be reviewed by the end of that year

the beginning of the trip, signing it in at the end of the trip and lockable storage for the duration of the trip.

Data Protection by Design

Whenever a new policy, procedure, system or database involving personal data is proposed a Privacy Impact Assessment will be completed. This will be used to identify and reduce any risks to privacy and potential risks of harm to individuals through the misuse of their personal information

Data Subjects' Rights

Any person wishing to exercise their rights under data protection legislation can do so by writing to the contact details below. Details of our approach to information requests can be found in Appendix 1. Further detail of data subjects' rights can be found in Appendix 9.

Breaches Of Data Protection

The school has a data breach management process which all staff are aware of and have received appropriate training to help them recognise and react appropriately to data breaches. All breaches or suspected breaches of Data Protection legislation will be reported to the school's Data Protection Lead who will ensure the process is adhered to and ensure breaches are reported to the ICO where necessary.

Information Security

This policy contains all reference to things traditionally covered in an Information Security Policy, covering the creation, acquisition, retention, transit, use, and disposal of all forms of information.

It applies to all employees and School Governors; it also applies to volunteers, work experience candidates, and all staff of service delivery partners and other organisations who handle information for which the school is responsible. It will form the basis of contractual responsibilities in contracts with Data Processors where reference is made to the school's Data Protection and Information Security Policy.

It is the policy of the School that:

- we will protect information from a loss of:
    - confidentiality (ensuring information is accessible only to authorised individuals)
    - integrity (safeguarding the accuracy and completeness of information)
    - availability (ensuring that authorised users have access to relevant information when required)
    - relevance (only keeping what we need for as long as it is needed)
- we will meet all regulatory and legislative information management requirements
- we will maintain business continuity plans
- we will deliver appropriate information security training to all staff
- we will make available appropriate and secure tools to all staff

- we will report and follow-up all breaches of information security, actual or suspected

Guidance and procedures will be maintained to support this policy. These will include procedural standards for individuals with access to information. System operating procedures will be developed and maintained to ensure compliance with this policy. Information systems are checked regularly for technical compliance with relevant security implementation standards. Operational systems are subjected to technical examination to ensure that hardware and software controls have been correctly implemented.

Management of Information

The School will manage information in accordance with the principles and procedures within this policy and other relevant policies and standards. The following principles apply to how we handle information in the school:

- All identifiable personal information is treated as confidential and will be handled in accordance with the relevant legal and regulatory protocols.
- All identifiable information relating to staff is confidential except where national policy on accountability and openness requires otherwise.
- Procedures will be maintained to ensure compliance with Data Protection legislation, The Human Rights Act 1998, the common law duty of confidentiality, the Freedom of Information Act 2000 and any other relevant legislation or statutory obligation.
- Information is recorded, used and stored to protect integrity so that it remains accurate and relevant at all times.

School Records

We will create and maintain adequate pupil, staff and other records to meet the school's business needs and to account fully and transparently for all actions and decisions. Such records can be used to provide credible and authoritative evidence where required; protect legal and other rights of the school, its staff and those who have dealings with the school; facilitate audit; and fulfil the school's legal and statutory obligations. Records will be managed and controlled effectively to fulfil legal, operational and information needs and obligations in the most cost-effective manner, in line with the school's Records Management policy.

Complaints

Complaints about the above procedures should be made to the Chairperson of the Governing Body who will decide whether it is appropriate for the complaint to be dealt with in accordance with the College's complaint procedure. Complaints will be dealt with in accordance with the College's complaints policy. Complaints which are not appropriate to be dealt with through the College's complaint procedure can be dealt with by the Information Commissioner. Contact details of both will be provided with any disclosure information

Contacts

If you have any enquires in relation to this policy, for a subject access request or concerns about how we handle data, in the first instance, use the following contact details.

The Head Teacher / Data Protection Lead
Heathfield Community College
Cade St
Heathfield
East Sussex
TN21 8RJ
Tel: 01435 866066

Data Protection Officer contact details: Peter Questier, Children's Services, East Sussex County Council.

Further advice and information is available from the Information Commissioner's Office:

The Information Commissioners
Wycliffe House
Water Lane
Wilmslow
Cheshire SK9 5AF

website: www.ico.gov.uk or telephone 01625 545745 3

Appendix 1: Freedom of Information Schedule

Rights of access to information

There are two distinct rights of access to information held by Colleges about pupils.

1. Under the GDPR (2018) & the Data Protection Act (2018) any individual has the right to make a request to access the personal information held about them.
2. The right of those entitled to have access to curricular and educational records is as defined within the Education Pupil Information (Wales) Regulations 2004.

These procedures relate to subject access requests made under the GDPR (2018) & the Data Protection Act (2018). They apply UNLESS such access is prevented by a court order.

Actioning an access request

1. Requests for information must be made in writing; which includes email, and be addressed to the Headteacher AND copied to the Data Protection Lead. If the initial request does not clearly identify the information required, then further enquiries will be made. The one calendar month time limit on responding to any such enquiry does not begin until the information required is clear.
2. The identity of the requestor must be established before the disclosure of any information, and checks should also be carried out regarding proof of the relationship to the child concerned. The one calendar month time limit on responding to any such enquiry does not begin until evidence of identity can be established by requesting production of TWO of the following
   - passport
   - driving licence
   - utility bills with the current address
   - Birth / Marriage certificate
   - P45/P60
   - Credit Card or Mortgage statement

3. Any individual has the right of access to information held about them if they are over the age of 16. Parents of children under the age of 16 have the right to access the "Educational record" of their child regardless of the child's age. Parents do not have the right to access other information held about their children unless the child gives their consent OR the child is not considered to have a capacity to understand such as request. GDPR requires the age, for which pupils must be asked to give their consent to parents seeing all of their data, to be 13, dependent upon the pupil's capacity to understand (which is normally considered to be age 12 or above or as judged according to the individual neds of the student – the latter is at the discretion of the Head Teacher). Regardless of age, the Head Teacher should discuss the request with the child and MUST take their views into account when making a decision. A child with competency to understand **can** refuse to consent to the request for their non "educational record" AND they must be asked for explicit written consent before complying with a request about them. Where the child is not deemed to be competent an individual with parental responsibility or guardian shall make the decision on behalf of the child.

4. The College may make a charge for the provision of information, dependent upon the following:
    - Charges can only be made if the information is provided in hard copy format & if the information requested contains the educational record then the amount charged will be dependent upon the number of pages provided.
    - If the information requested is to be provided in electronic format there will be no charge made unless the request is excessive or repetitive, in which case we will charge an amount that reflects the quantity of the information requested, taking into account the administrative costs of complying with the request.

5. The response time for subject access requests, once officially received, is 15 days for pupils to see the information that is held about their educational record and ONE calendar month **(irrespective of College holiday periods)** for other requests, UNLESS the request is complex (or if multiple requests are received from the same person). However, the ONE calendar month will not commence until after receipt of fees or clarification of information is sought and received. Complex requests will be complied with within 3 months and the applicant will be informed of the delay within the initial one month period. A request is considered complex if:
    - it involves retrieval and appraisal of information from multiple sources
    - it involves the retrieval of large volumes of information for one data subject
    - which are difficult to separate from information relating to other data subjects
    - it is one in a series of requests from the same individual
    - it involves the release of third party data for which consent has been refused or cannot be obtained

6. The GDPR (2018) & the Data Protection Act (2018) allows exemptions as to the provision of some information; **therefore, all information will be reviewed prior to disclosure**.

7. Third party information is that which has been provided by another, such as the Police, Local Authority, Health Care professional or another College. Before disclosing third party information consent should be obtained. There is still a need to adhere to the ONE calendar month statutory timescale.

8. Any information which may cause serious harm to the physical or mental health or emotional condition of the pupil or another should not be disclosed, nor should information that would reveal that the child is at risk of abuse, or information relating to court proceedings.

9. If there are concerns over the disclosure of information then additional advice should be sought.

10. Where redaction (information blacked out/removed) has taken place then a full copy of the information provided should be retained in order to establish, if a complaint is made, what was redacted and why.

11. Information disclosed should be clear, thus any codes or technical terms will need to be clarified and explained. If information contained within the disclosure is difficult to read or illegible, then it should be retyped.

12. Information can be provided at the College with a member of staff on hand to help and explain matters if requested, or provided at face to face handover. The views of the applicant should be taken into account when considering the method of delivery. If postal systems have to be used then registered/recorded mail **must** be used.

Appendix 2: Moving Information

Transferring confidential information

When removing special categories of personal data or confidential information from College premises, you must use the most secure method available. The method chosen will depend on the circumstances and should be based on:

- the amount of data
- the impact on individuals and the College of losing the data
- the level of risk of losing the data
- the urgency of the data transfer.

Electronic transfer is often the quickest way of sending large amounts of confidential data to other agencies. It CAN also be the safest way of transferring highly sensitive information from College premises.

Transferring confidential information securely

When needing to transfer confidential information, the College will:

- Use an approved secure transfer mechanism to send confidential information to other agencies. For example, we can use AVCO or s2s for sending and receiving confidential files from East Sussex County Council (ESCC) or other Colleges.
- Use secure (internal) email for sending emails with confidential information to Heathfield Community College email addresses.
- If secure email is not available, encrypt confidential information using encryption software before emailing it to other agencies. See our page on email security.
- Use only encrypted laptops or memory sticks, if using them for carrying special categories of personal data or confidential information. We will never carry such information on unencrypted electronic media.
- Use Royal Mail signed-for delivery (recorded or special delivery) or a trusted courier for posting highly sensitive information.
- Use fax for sending or receiving special categories of personal data or confidential information only if the need is urgent and there is no more secure alternative available.
- Transfer only as much information as is necessary for the purpose.

Carrying paper records containing confidential information

When there is a need to carry paper records, containing confidential information, we / person involved will:

- Ensure that there is no other more secure option, such as electronic transfer.
- Never take an original file or document, if it is practical to make and carry a copy.
- Take records out of their secure location only for as long as is necessary and transfer them back to their secure location as soon as possible.
- Only carry confidential records in a secure briefcase or container.
- Keep the information on their person whenever possible and lock it away securely when it is not possible. We will NEVER leave the information in plain sight in public places.

- Ensure, when confidential information is being transported by car, that it is locked in the car boot.
- Keep records secure and confidential while at home. NEVER allow family members, friends or colleagues to see the contents or the outside folder of the records.

Appendix 3: The Heathfield Community College Freedom of Information Publication Scheme

This publication scheme is based on but has been adapted from the model scheme published by the Information Commissioner.

This publication scheme commits the College to make that information, required by law, available to the public as part of its normal activities. The information covered is included in the classes of information mentioned below, where this information is held by the College.

The scheme commits the college:

- To proactively publish or otherwise make available as a matter of routine, information, including environmental information, which is held by the College and falls within the classifications below.
- To specify the information, which is held by the College and falls within the classifications below.
- To proactively publish or otherwise make available as a matter of routine, information in line with the statements contained within this scheme.
- To produce and publish the methods by which the specific information is made routinely available so that it can be easily identified and accessed by members of the public.
- To review and update on a regular basis the information the College makes available under this scheme.
- To produce a schedule of any fees charged for access to information which is made proactively available.
- To make this publication scheme available to the public.
- To publish any dataset held by the College that has been requested, and any updated versions it holds, unless the College is satisfied that it is not appropriate to do so; to publish the dataset, where reasonably practicable, in an electronic form that is capable of re-use; and, if any information in the dataset is a relevant copyright work and the public authority is the only owner, to make the information available for re-use under a specified licence. The term ‘dataset’ is defined in section 11(5) of the Freedom of Information Act. The terms ‘relevant copyright work’ and ‘specified licence’ are defined in section 19(8) of that Act.

Classes of information

Who we are and what we do

- Organisational information, locations and contacts, constitutional and legal governance.

What we spend and how we spend it

- Financial information relating to projected and actual income and expenditure, tendering, procurement and contracts.

What our priorities are and how we are doing

- Strategy and performance information, plans, assessments, inspections and reviews.

How we make decisions

- Policy proposals and decisions. Decision making processes, internal criteria and procedures, consultations.

Our policies and procedures

- Current written protocols for delivering our functions and responsibilities.

Lists and registers

- Information held in registers required by law and other lists and registers relating to the functions of the College.

The services we offer

- Advice and guidance, booklets and leaflets, transactions and media releases. A description of the services offered.

The classes of information will not generally include:

- Information the disclosure of which is prevented by law, or exempt under the Freedom of Information Act, or is otherwise properly considered to be protected from disclosure.
- Information in draft form.
- Information that is no longer readily available as it is contained in files that have been placed in archive storage, or is difficult to access for similar reasons.

The method by which information published under this scheme will be made available

- The authority will indicate clearly to the public what information is covered by this scheme and how it can be obtained.
- Where it is within the capability of the College, information will be provided on our website. Where it is impracticable to make information available on the website or when an individual does not wish to access the information by the website, the college will indicate how information can be obtained by other means and provide it by those means.
- In exceptional circumstances some information may be available only by viewing in person. Where this manner is specified, contact details will be provided. An appointment to view the information will be arranged within a reasonable timescale.

- Information will be provided in the language in which it is held or in such other language that is legally required.
- Obligations under disability and discrimination legislation and any other legislation to provide information in other forms and formats will be adhered to when providing information in accordance with this scheme.
- Charges which may be made for information published under this scheme. The purpose of this scheme is to make the maximum amount of information readily available at minimum inconvenience and cost to the public. Charges made by the College for routinely published material will be justified and transparent and kept to a minimum.
- Material which is published and accessed on a website will be provided free of charge. Charges may be made for actual disbursements incurred such as:
    - photocopying
    - postage and packaging
    - the costs directly incurred as a result of viewing information
- Charges may also be made for information provided under this scheme where they are legally authorised, they are in all the circumstances, including the general principles of the right of access to information held by the College, justified and are in accordance with a published schedule or schedules of fees which is readily available to the public.
- Charges may also be made for making datasets (or parts of datasets) that are relevant copyright works available for re-use. These charges will be in accordance with either regulations made under section 11B of the Freedom of Information Act or other enactments.

Appendix 4: Consent

Where consent is considered to be the legal justification for a data processing activity or other activity, there are exemptions to the requirement to seek explicit parental consent:

- the parent cannot be found, for example, his or her whereabouts or identity is not known and there is documentary evidence of reasonable attempts made to contact the parent
- the parent lacks the mental capacity[5] to object or to consent;
- the welfare of the child requires that a particular parent is not contacted, for example where a child has been separated from an abusive parent who is not to be informed of the child's whereabouts; or
- where it is otherwise not reasonably practicable for a particular parent to be notified or for his or her consent to be obtained.

Seeking Consent for Children whose parents cannot be notified as outlined in the Protection of Freedoms Act 2012

a) if the child is being 'looked after' by a local authority or is accommodated or maintained by a voluntary organisation (i.e. a not-for-profit organisation), the local authority, or as the case may be, the voluntary organisation must be notified and their written consent obtained.
b) if paragraph a) above does not apply, then notification must be sent to all those caring for the child and written consent must be gained from at least one carer before the child's biometric data can be processed (subject to the child and none of the carers objecting in writing).
c) If paragraph b) applies & the school does not have the contact details of both parents, then the school will decide whether any "reasonable steps" can or should be taken to ascertain the details of the other parent

[5] Within the meaning of the Mental Capacity Act 2005

Appendix 5: Biometric Data

Biometric Information is information about a person's physical or behavioural characteristics than can be used to identify them, for example, information from their fingerprint. The college would like to use information from a person's fingerprint and use this information for the purposes of providing automated systems, such as a cashless payment system for food in the College. It is possible that in the future this may be extended to other systems. If this happens, parents will be informed in advance.

The information will be used as part of an automated biometric recognition system. This system will take measurements of a fingerprint and convert these measurements into a template to be stored on the system. An image of fingerprint is **not** stored. The template (i.e. measurements taking from a fingerprint) is what will be used to permit access to services.

It should be noted that the law places specific requirements on schools when using personal information, such as biometric information, about pupils for the purposes of an automated biometric recognition system. For example:

a) The school cannot use the information for any purpose other than those for which it was originally obtained and made known to parents i.e. as stated above; b) the school must ensure that the information is stored securely;
c) the school must inform what it intends to do with the information;
d) unless the law allows it, the school cannot disclose personal information to another person/body.

The law says that schools must provide reasonable alternative arrangements for children who are not going to use the automated system and details of this will be communicated to parents when they are asked for their consent.

When a child leaves the school, or if for some other reason he / she ceases to use the biometric system, his / her biometric data will be securely deleted.

Appendix 6: Privacy Notices

There are privacy notices for each of the following stakeholder groups:

- Pupils
- Parents of pupils, regarding pupil data
- Parents of pupils, regarding parental data
- College workforce
- Governors
- Lettings and other customers of the college
- Alumni

These can be found on the policies page of the College website, located in the Data Protection materials, at the following URL:

http://www.heathfieldcc.co.uk/?page_id=410816

Heathfield Community College Data Protection Policy, Incorporating the Freedom of Information Schedule & The College Records Management Policy

Appendix 7: College Records Management Policy

Heathfield Community College will create and maintain adequate pupil, staff and other records to meet the school's business needs and to account fully and transparently for all actions and decisions. Such records can be used to provide credible and authoritative evidence where required; protect legal and other rights of the school, its staff and those who have dealings with the school; facilitate audit; and fulfil the school's legal and statutory obligations.

Records provide evidence for protecting the legal rights and interests of the school, and provide evidence for demonstrating performance and accountability. This document provides the policy framework through which this effective management can be achieved and audited. It covers:

- Scope
- Responsibilities
- Relationships with existing policies

1. Scope of the policy

    1.1 This policy applies to all records created, received or maintained by staff of the college in the course of carrying out its functions.

    1.2 Records are defined as all those documents which facilitate the business carried out by the college and which are thereafter retained (for a set period) to provide evidence of its transactions or activities. These records may be created, received or maintained in hard copy or electronically.

    1.3 A small percentage of the college's records will be selected for permanent preservation as part of the institution's archives and for historical research. This should be done in liaison with the County Archives Service.

2. Responsibilities

    2.1 The college has a corporate responsibility to maintain its records and record keeping systems in accordance with the regulatory environment. The person with overall responsibility for this policy is the Head Teacher.

    2.2 The person responsible for records management in the school will give guidance for good records management practice and will promote compliance with this policy so that information will be retrieved easily, appropriately and in a timely way. They will also monitor compliance with this policy by surveying at least annually to check if records are stored securely and can be accessed appropriately.

    2.3 Individual staff and employees must ensure that records for which they are responsible are accurate, and are maintained and disposed of in accordance with the college's records management guidelines.

3. Relationship with existing policies

    This policy has been drawn up within the context of:

    - Freedom of Information policy
    - Data Protection policy
    - and with other legislation or regulations (including audit, equal opportunities and ethics) affecting the school.

Appendix 8: Pupil Records & The Retention Schedule

The Pupil Record:
Items which should be included on the pupil record:

- Admission form (application form)
- Privacy Notice [only the most recent needs be on the file]
- Photography & other consents
- Years Record
- Annual Written Report to Parents
- National Curriculum and RE Locally Agreed Syllabus Record Sheets
- Information relating to major incidents (either an accident or other incident)
- Reports written about the child, internal & external examination results
- Information about an EHCP / statement & support offered in relation to the EHCP /Statement; including reviews, advice, accessibility strategies.
- Medical information (stored in the file in a clearly marked sealed envelope)
- Child protection reports/disclosures (if stored in hard copy they should be clearly marked and in a sealed envelope). In subject Access Requests these may be redacted if their disclosure could lead to harm.
- Any information relating to exclusions (fixed or permanent)
- Any correspondence with parents or outside agencies relating to major issues
- Details of any complaints made by the parents or the pupil
- Pupil premium/ sixth form bursary
- FSM, evidence of eligibility
- Statistics and management information, including courses taken, exam entries, MIS marksheets

Other Records about Pupils
The following records should be stored separately to the pupil record as they are subject to shorter retention periods and if they are placed on the file then it will involve a lot of unnecessary weeding of the files once the pupil leaves the school.

- Absence notes
- Parental consent forms for trips/outings [in the event of a major incident all the parental consent forms should be retained with the incident report not in the pupil record]
- Correspondence with parents about minor issues
- Accident forms (these should be stored separately and retained on the school premises until their statutory retention period is reached. A copy could be placed on the pupil file in the event of a major incident)
- Census returns, attendance returns to the Local Authority
- Returns made to the DfE
- Census returns, attendance returns to the Local Authority

Retention

The College will retain the pupil record of every student that has been on the College roll until the pupil reaches the age of 25 years UNLESS the pupil has been subject to child protection procedures, in which case it will be retained indefinitely, or unless our published retention schedule specifies otherwise. A copy of the retention schedule can

be found on the policies page of the College website, located in the Data Protection materials, at the following URL:

http://www.heathfieldcc.co.uk/?page_id=410816

Safe destruction of the pupil record

The pupil record should be disposed of in accordance with the safe disposal of records guidelines. The Freedom of Information Act 2000 requires the college to maintain a list of records which have been destroyed and who authorised their destruction. Members of staff should record at least:

- File reference (or other unique identifier);
- File title (or brief description);
- Number of files and date range
- The name of the authorising officer
- Date action taken

.

Transfer of a pupil record outside the UK

If we are requested to transfer a pupil file outside of the UK because a pupil has moved into out of the UK, we will contact the Local Authority for further advice before doing so. However, the general principle that we will follow is that the educational record requires the parent's consent for us to do so and other data outside of the educational record requires the pupil's consent for us to do so.

Appendix 9: Data Subjects' Rights

Right of Access

Under data protection legislation every individual has the right of access to information relating to them. This right is called Subject Access. Any person wishing to make a Subject Access request can do so by following the instructions above. Personal information will never be disclosed verbally in response to a request.

Written consent will always be required from any person nominating a third party to request information on their behalf. Parents may make requests on behalf of their children but if the child is 13 years or older, the child must also provide written consent for the parent to make the application on their behalf.

A nominated person may make an application on behalf of anyone lacking mental capacity who would otherwise have the right to request access to their records. In these circumstances, the person making the application must have proof of a valid Lasting Power of Attorney or an Enduring Power of Attorney or proof of Court-appointed Deputyship.

No information relating to any other person (other than the individual requesting the information) will be disclosed as part of a subject access disclosure.

Any information that may prejudice the prevention and detection of crime may be exempted from disclosure. There are also a number of other exemptions which may be applied and these will be explained on an individual basis.

Right of erasure

This right allows individuals to request that their personal data is deleted where there is no justification for its continued use. It only applies, however, when:

1. The data is no longer necessary for the reason(s) for which it was originally collected
2. The data subject provided consent for the school to process their data but has subsequently withdrawn this consent
3. That data subject has objected to the school processing their data and there are no overriding grounds for continuing to process it
4. The data was processed in breach of the GDPR i.e. it was unlawfully processed
5. There is a legal requirement to erase the data
6. The data was collected with parental consent when the data subject was a child and they no longer wish for their data to be held

The school will also decline a request for erasure:

1. When we have a legal obligation or it is part of our official authority to process the data
2. For public health reasons

3. For certain archiving activities
4. When we need the data in connection with a legal claim

Right to rectification

If data subjects believe that any of the personal data the school holds about them is inaccurate or incomplete they are entitled to ask for it to be rectified. This will be looked at in the context of why the school is processing the information any necessary steps will be taken to supplement the information held in order to make it complete.

Right to restriction

In certain circumstances data subjects have a right to request that we temporarily restrict processing and access to their data. This will apply:

1. Whilst establishing accuracy of data, if a data subject has contested this
2. Whilst we follow up any objection raised by a data subject to the school processing their data.
3. When data has been processed unlawfully but the data subject does not want us to erase it and have asked, instead, for us to restrict processing of the data.
4. When we no longer need the data but the data subject has advised us that they need it in connection with a legal claim.

The right to restrict data doesn't apply if:

1. The processing is necessary for the school in connection with a legal claim
2. It is necessary for the protection of another person
3. There are substantial public interest reasons for continuing to process the data

Right to portability

Data subjects have a right to request that their data be transferred electronically to another organisation.

This only applies when:

1. The data subject themselves supplied the information and provided consent for the processing; or
2. The data is being processed as part of a contract to which the data subject is party; and
3. The data is held electronically (not in paper files)

Right to object

Data subjects have the right to object to their information being processed in the following circumstances:

- If the school has decided that processing is necessary either to
  a) perform a task carried out in the public interest or
  b) as part of the school's official authority or legitimate interest and the data subject feels this is not applicable.
  Information about why the school is processing information (the legal justification) can be found in the school's privacy notice.
- If the school retains information in defence or potential defence of a legal claim but the data subject believes there are insufficient grounds to do so.

Data subjects also have a right to object to their data being used for direct marketing purposes at any time and the school will cease processing for this purpose if an objection is raised.

If the school uses IT systems to make automatic decisions based on personal data individuals have a right to object and:

- request human intervention in the decision making
- be able to express their point of view
- obtain an explanation of how a decision has been reached
- challenge the decision

This right does not exist if the automated decision making:

- is necessary to fulfil a contract to which they are party
- is authorised by law
- the data subject has consented to the processing

Individuals also have the right to object to data being used for research purposes unless the research is being undertaken in the wider public interest which outweighs a data subject's right to privacy.

Right to be Informed

The school issues a privacy notice which explains what information the school is processing, the legal basis for this, the purpose of processing, who the information is shared with and other information required by data protection legislation. The current privacy notice is available on the school's website: (http://www.heathfieldcc.co.uk/?page_id=1595711) or on written request from the contact details in this policy above.