Framlingham
Sir Robert Hitcham's
CEVAP School

College Road Framlingham
Woodbridge Suffolk IP13 9EP
01728 723354
www.hitchamsframlingham.org.uk

Statutory Policy

Data Protection

Adopted from the Schools' Choice GDPR template

January 2025

Committee **Whole Governing Body**

Headteacher Mrs L Cann (NPQH; BSc Hons; PGCE)
Deputy Mrs E Hall (BEd Hons; PGCE)
Email admin@hitchams.suffolk.sch.uk

Related Policies

The School also adopts the following polices that relate to the Data Protection Policy:

- Information Management & Security Policy which includes:
- Acceptable Use and Digital Images
- CPD / Staff Induction
- Staff / Volunteer Code of Conduct
- Confidentiality
- Data Retention Schedule (Appendix A)

Introduction

The school is committed to being transparent about how it collects and uses the personal data of its staff, children, parents and carers, and to meeting its data protection obligations.

This policy sets out the school's commitment to data protection, and individual rights and obligations in relation to personal data.

The school has appointed School's Choice Data Protection Team, as its data protection officer. Their role is to inform and advise the school on its data protection obligations.

They can be contacted at Schools' Choice Tel: 01473 260700 email: data.protection@schoolschoice.org and questions about this policy, or requests for further information, should be directed to them.

Definitions

Personal data – any information that relates to an individual who can be identified from that information.

Processing – any use that is made of data, including collecting, storing, amending, disclosing or destroying it.

Special categories of personal data – means information about an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life or sexual orientation and biometric data.

Criminal records data – means information about an individual's criminal convictions and offences, and information relating to criminal allegations and proceedings.

Data Protection Principles

The school processes personal data in accordance with the following data protection principles:

- The school processes personal data lawfully, fairly and in a transparent manner.
- The school collects personal data only for specified, explicit and legitimate purposes.
- The school processes personal data only where it is adequate, relevant and limited to what is necessary for the purposes of processing.
- The school keeps accurate personal data and takes all reasonable steps to ensure that inaccurate personal data is rectified or deleted without delay.
- The school keeps personal data only for the period necessary for processing.
- The school adopts appropriate measures to make sure that personal data is secure, and protected against unauthorised or unlawful processing, and accidental loss, destruction or damage.

The school tells individuals the reasons for processing their personal data, how it uses such data and the legal basis for processing in its privacy notices. It will not process personal data of individuals for other reasons.

Where the school processes special categories of personal data or criminal records data to perform obligations or to exercise rights in employment law, this is done in accordance with the General Data Protection Regulation (GDPR).

The school will update personal data promptly if an individual advises that their information has changed or is inaccurate and data gathered is held in:

- the individual's personnel file (in hard copy or electronic format, or both)
- on HR systems
- in child files
- on systems as appropriate (SIMs.net, ParentMail, Cornerstones, Tapestry, Governor Hub)

The periods for which the school holds personal data are contained in its privacy notices/retention schedule and the school keeps a record of its processing activities in respect of personal data in accordance with the requirements of the General Data Protection Regulation (GDPR).

Privacy Notices

The school has a duty to check that staff, children, parents and carers information is accurate and up to date. It fulfils this by sending out a data collection form to parents/carers/staff on an annual basis.

This form will also include a privacy notice which outlines:

- who we are (including our contact details);
- the contact details of our Data Protection Officer;
- the purpose of the school processing data;
- the legal basis for processing data; and
- who this data will be shared with.

The current privacy notices for each relevant category of data subjects can be found in the school office in the GDPR file, on the office server and selected notices are also posted on the school website.

Data Retention

The school maintains a retention schedule which can be found in Appendix A of this policy or at the school office in the GDPR file & on the office server.

This retention schedule is based on guidance from the information and records management society: http://www.irms.org.uk/resources/information-guides/199-rm-toolkit-for-school and it encompasses records managed by all types of school – some of the file descriptions listed may not be relevant to every school.

Individual Rights

As a data subject, individuals have a number of rights in relation to their personal data.

Subject Access Requests

Individuals have the right to make a subject access request. If an individual makes a subject access request, the school will tell them:

- whether or not their data is processed and if so why, the categories of personal data concerned and the source of the data if it is not collected from the individual;
- to whom their data is or may be disclosed, including to recipients located outside the European Economic Area (EEA) and the safeguards that apply to such transfers;
- for how long their personal data is stored (or how that period is decided);
- their rights to rectification or erasure of data, or to restrict or object to processing;
- their right to complain to the Information Commissioner if they think the school has failed to comply with their data protection rights; and
- whether or not the school carries out automated decision-making and the logic involved in any such decision-making (i.e. e-recruitment software.)

The school will also provide the individual with a copy of the personal data undergoing processing. This will normally be in electronic form if the individual has made a request electronically, unless they agree otherwise.

To make a subject access request, the individual should complete the relevant form/send the request to admin@hitchams.suffolk.sch.uk In some cases, the school may need to ask for proof of identification before the request can be processed. The school will inform the individual if it needs to verify their identity and the documents it requires.

The school will normally respond to a request within a period of one month from the date it is received. In some cases, such as where the school processes large amounts of the individual's data, it may respond within three months of the date the request is received. The school will write to the individual within one month of receiving the original request to tell them if this is the case.

If a subject access request is manifestly unfounded or excessive, the school is not obliged to comply with it. Alternatively, the school can agree to respond but will charge a fee, which will be based on the administrative cost of responding to the request. A subject access request is likely to be manifestly unfounded or excessive where it repeats a request to which the school has already responded. If an individual submits a request that is unfounded or excessive, the school will notify them that this is the case and whether or not it will respond to it.

Other Rights

Individuals have a number of other rights in relation to their personal data. They can require the school to:

- rectify inaccurate data;
- stop processing or erase data that is no longer necessary for the purposes of processing;
- stop processing or erase data if the individual's interests override the school's legitimate grounds for processing data (where the school relies on its legitimate interests as a reason for processing data);
- stop processing or erase data if processing is unlawful; and
- stop processing data for a period if data is inaccurate or if there is a dispute about whether or not the individual's interests override the school legitimate grounds for processing data.

To ask the school to take any of these steps, the individual should send the request to admin@hitchams.suffolk.sch.uk

Disclosure of Personal Information

Information Sharing with Professionals Working with Children

Information sharing between professionals is vital to ensure the wellbeing of Children.

The school will follow the "7 golden rules of Information Sharing" described by the DfE:

1. Remember that the DPA/GDPR is not a barrier to sharing information
2. Be open and honest with the person or family
3. Seek advice if you are in any doubt
4. Share with consent where appropriate
5. Consider safety and well-being
6. Necessary, proportionate, relevant, accurate timely, and secure
7. Keep a record of your decision and reasons

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/419628/Information_sharing_advice_safeguarding_practitioners.pdf

Access to Pupils Records

Parents have two distinct rights to access information about their child held by a school.

These rights are:

1. The parent's right of access to their child's educational record under The Education (Pupil Information) Regulations 2005. A link to this document can be found here. http://www.legislation.gov.uk/uksi/2005/1437/contents/made
2. The pupil's right of subject access

A child or young person will always be the owner of their personal information however if a young person is incapable of making their own decisions which is generally accepted as under the age of 12, the primary carer or guardian would act on their behalf. This authority is only extended to functions that are in the 'best interests' of the child or young person.

The school will respond to a subject access request within 1 calendar month. If this request comes from someone other than the individual, the school will consider the capability of the individual and also must ensure the requester is acting the in the best interests of the individual.

Requests for information from pupils, or parents, for information that contains, wholly or partly, an educational record must receive a response within 15 school days.

Under the Regulations, requests from parents to view their child's educational record will be dealt with by the Board of Governors. All other requests for personal information from the pupil, or someone acting on their behalf, will be dealt with by the Head Teacher on behalf of the school.

International Data Transfers

The school will not transfer personal data to countries outside the EEA.

Freedom of Information/Environmental Information Regulations

The school as a public authority is subject to The Freedom of Information Act 2000 (FOI) and Environmental Information Regulations 2004 (EIR) and all requests for information that is not personal information must be treated as a FOI or EIR. These requests must be fully responded within 20 (school) working days by law. The information will be provided unless the school can provide an exemption or exception under the FOI act or EIR respectively.

In line with FOI the school is required to have a **Publication Scheme** showing what information is held and how you can access this. The school's publication scheme can be found in the school office GDPR file & on the office server.

Data Security

The school takes the security of personal data seriously. The school has internal policies and controls in place to protect personal data against loss, accidental destruction, misuse or disclosure, and to ensure that data is not accessed, except by employees in the proper performance of their duties.

Internal policies and controls include: systems that are user restricted; systems with username/password access only; all pcs/laptops are username/password restricted; all staff laptops are encrypted; all memory sticks are encrypted; all sensitive personal data is secured in locked cabinets/rooms in alarmed premises overnight/during holidays.

Where the school engages third parties to process personal data on its behalf, such parties do so on the basis of written instructions, are under a duty of confidentiality and are obliged to implement appropriate technical and organisational measures to ensure the security of data.

An Information Risk Register is maintained by the school which summarises each information asset the school maintains. Appropriate measures will be taken to mitigate the risk of disclosure of each information asset based on the impact level assigned. The information risk register can be found in the school office GDPR file & on the office server.

Artificial Intelligence

Artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Bard. Framlingham Sir Robert Hitcham's school recognises that AI has many uses to help pupils learn, but also poses risks to sensitive and personal data.

To ensure that personal and sensitive data remains secure, no one will be permitted to enter such data into unauthorised generative AI tools or chatbots.

If personal and/or sensitive data is entered into an unauthorised generative AI tool, Framlingham Sir Robert Hitcham's school will treat this as a data breach, and will follow the personal data breach procedure outlined below.

Privacy Impact Assessments

Some of the processing that the school carries out may result in risks to privacy. Where processing would result in a high risk to individual's rights and freedoms, the school will carry out a data privacy impact assessment to determine the necessity and proportionality of processing. This will include considering the purposes for which the activity is carried out, the risks for individuals and the measures that can be put in place to mitigate those risks

Data Breaches

If the school discovers that there has been a breach of personal data that poses a risk to the rights and freedoms of individuals, it will report it immediately to our School's Choice Data Protection officer who in turn will report it to the Information Commissioner within 72 hours of discovery. The school will record all data breaches regardless of their effect.

If the breach is likely to result in a high risk to the rights and freedoms of individuals, it will tell affected individuals that there has been a breach and provide them with information about its likely consequences and the mitigation measures it has taken.

Individual Responsibilities

Individuals are responsible for helping the school keep their personal data up to date. Individuals should let the school know if data provided to the school changes, for example if an individual moves house.

Individuals may have access to the personal data of other individuals in the course of their employment. Where this is the case, the school relies on individuals to help meet its data protection obligations.

Individuals who have access to personal data are required:

- to access only data that they have authority to access and only for authorised purposes;
- not to disclose data except to individuals (whether inside or outside the school) who have appropriate authorisation;
- to keep data secure (for example by complying with rules on access to premises, computer access, including password protection, and secure file storage and destruction);
- not to remove personal data, or devices containing or that can be used to access personal data, from the school's premises without adopting appropriate security measures (such as encryption or password protection) to secure the data and the device.

Failing to observe these requirements may amount to a disciplinary offence, which will be dealt with under the school's disciplinary procedure. Significant or deliberate breaches of this policy, such as accessing data without authorisation or a legitimate reason to do so, may constitute gross misconduct and could lead to dismissal without notice.

Training

The school will provide training to all individuals about their data protection responsibilities as part of the induction process and at regular intervals thereafter.

Individuals whose roles require regular access to personal data, or who are responsible for implementing this policy or responding to subject access requests under this policy, will receive additional training to help them understand their duties and how to comply with them.

Roles and Responsibilities

The senior information risk owner (SIRO) for the school is the headteacher.

They are responsible for:

- Owning and updating this policy
- Owning the risk register
- Advocating information risk management and raising awareness of information security issues

All staff are responsible for ensuring that information is managed according to this policy.