Hillcross Primary School

Data Protection Policy

Contents

Introduction

Under UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA), schools have to:

- comply with the legislation
- demonstrate that they're complying

It's a legal requirement that your school has data protection policies and procedures in place and that you regularly review and update these, along with the associated documentation. You should also review your other statutory policies in the light of data protection legislation.

Hillcross Primary School

Hillcross Primary School is committed to being transparent about how it collects and uses data in order to meet its data protection obligations. This policy sets out our commitment to the protection of data. Please also refer to our HR related policy for specific guidance on the personal data of job applicants, employees, workers, contractors, volunteers, interns, apprentices and former employees. We may, from time to time, be required to share personal information about employees, pupils, students or trainees with other organisations, this includes Local Authorities, Department for Education, other schools and educational bodies, and potentially social services and law enforcement agencies.

This policy is in place to ensure all staff and governors are aware of their responsibilities and outlines how we comply with the principles of the UK GDPR and Data Protection Act 2018. Organisational methods for keeping data secure are imperative, and we believe that it is good practice to keep clear practical policies, backed up by written procedures. We have signed up to Merton's Data Protection Officer Service Level Agreement. The role of the DPO is to inform and advise us on our data protection obligations. The DPO can be contacted at schoolsDPO@merton.gov.uk

Legal Framework

This policy has due regard to legislation, including, but not limited to the following:

- The UK General Data Protection Regulation (UK GDPR)
- The Data Protection Act 2018
- The Freedom of Information Act 2000
- The Education (Pupil Information) (England) Regulations 2005 (as amended in 2016)
- The Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004
- The School Standards and Framework Act 1998

This policy will also have regard to the following guidance:

- ICO (2021 Guide to the General Data Protection Regulation (UK GDPR)
- Department for Education 'Data Protection in Schools 2023', updated April 2024.

This policy will be implemented in conjunction with the following policies:

- Online-safety Policy
- Freedom of Information Policy
- The Use of Mobile Technology in School and Digital Images Policy
- Freedom of Information Policy and Model Publication Scheme
- Child Protection and Safeguarding Policy
- Records Management Policy

Hillcross Primary School is aware of the planned changes to legislation in the Data Protection and Digital Information Bill. The bill makes changes to the:

- UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- Privacy and Electronic Communications (EC Directive) Regulations 2003

What these changes mean

The changes include clearer guidance on sharing data for safeguarding purposes. It will be easier for people who care for children and vulnerable people to understand the legal requirements of sharing data.

Changes to the bill are in the early stages. DfE will share updates as it develops and provide guidance to help you perform your duties.

Applicable Data

Article 4 states that "'personal data' means any information relating to an identified or identifiable natural person ('data subject')".

An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person; The UK GDPR and Data Protection act 2018 applies to both automated personal data and to manual filing systems, where personal data is accessible according to specific criteria, as well as to chronologically ordered data and pseudonymised data.

Sensitive personal data is referred to in the UK GDPR as **'special categories of personal data'**, this is defined as:

- Genetic data
- Biometric data
- Data concerning health
- Data concerning a person's sex life
- Data concerning a person's sexual orientation
- Personal data which reveals:
    - Racial or ethnic origin
    - Political opinions
    - Religious or philosophical beliefs
    - Trade union membership

Principles

In accordance with the requirements outlined in the UK GDPR, personal data will be:

- Processed lawfully, fairly and in a transparent manner in relation to individuals.
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
- Accurate and, where necessary, kept up-to-date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods, insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to implementation of the appropriate technical and

organisational measures required by the UK GDPR and Data Protection Act 2018 in order to safeguard the rights and freedoms of individuals.

- Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

The UK GDPR also requires that "the controller shall be responsible for, and able to demonstrate, compliance with these principles".

Accountability and Responsibilities

Everyone in your school is responsible for protecting personal data. However, there are some key roles and responsibilities for data protection compliance.

The responsibility and accountability for compliance sits with governors. Schools risk getting a fine if they don't comply. Governors and trustees check that the school:

- monitors their data protection performance
- supports the data protection officer
- has good network security infrastructure to keep personal data protected
- has a business continuity plan in place that includes cyber security

Senior leaders are accountable for:

- deciding how the school uses technology and maintains its security
- deciding what data is shared and how
- setting school policies for the use of data and technology
- understanding what UK GDPR and the Data Protection Act covers and getting advice from the data protection officer, as appropriate
- assuring governors and trustees that the school has the right policies and procedures in place
- making sure any contracts with third-party data processors cover the relevant areas of data protection
- making sure staff receive training on data protection every 2 years (we recommend annually as best practice)

Staff training on data protection includes training on specific school processes such as:

- personal data breach reporting processes
- the escalation of information rights requests

All staff should be aware of what:

- personal data is
- 'processing' means
- their duties are in handling personal information
- the processes are for using personal information
- is permitted usage of that data
- the risks are if data gets into the wrong hands
- their responsibilities are when recognising and responding to a personal data breach
- the process is for recognising and escalating information rights requests

This includes teaching staff; catering staff; welfare supervisors; library staff; cleaners; first-aiders; governors and trustees; and volunteers.

There are extra requirements for any staff in school who:

- create and store data
- enter data into applications or software
- decide if and when they'll process certain data
- handle paper documents

Staff who collect, store or view personal data are responsible for:

- making sure they have a legitimate need to process the data
- checking that any data they store is needed to carry out necessary tasks
- identifying any risks
- understanding the governance arrangements that oversee the management of risks

Staff are responsible for making sure that pupils using personal data for projects or coursework do so appropriately. This includes being compliant when storing data.

The Information Commissioner's Office has guidance on training for staff. It also produces resources that we use to promote good data protection practice in your school.

This school will implement appropriate technical and organisational measures to demonstrate that data is processed in line with the principles set out in the UK GDPR. We will also provide comprehensive, clear and transparent privacy policies. Records of activities relating to higher risk processing will be maintained, such as the processing of special categories data or that in relation to criminal convictions and offences.

Internal records of processing activities will include the following:

- Name and details of the organisation
- Purpose(s) of the processing
- Description of the categories of individuals and personal data
- Retention schedules
- Categories of recipients of personal data
- Description of technical and organisational security measures
- Details of transfers to third countries, including documentation of the transfer mechanism and safeguards in place.

We will implement measures that meet the principles of data protection by design and data protection by default, such as:

- Data minimisation.
- Pseudonymisation.
- Transparency.
- Allowing individuals to monitor processing.
- Continuously creating and improving its security features.

Data protection impact assessments will also be used, where appropriate.

Hillcross Primary School

For most personal data, the school as an entity is the Data Controller, thus this role rests with the Headteacher and Governing body.

This means it's responsible under the Data Protection Act 2018 for protecting data in every situation where it decides:

- whose information to collect
- what types of data it needs
- why it needs it
- whether the information can be shared with a third party
- when and where data subjects' rights apply
- for how long to keep the data

As a data controller, we register with the Information Commissioner's Office.

Where, for example, a school is required to supply a copy of some personal data to the Department for Education (DfE), DfE also becomes an independent data controller of the copy it receives.

This school participates in the Merton Council **Data Protection Officer (DPO)** SLA which provides a shared DPO for Merton Schools. The individual appointed as DPO will have professional experience and knowledge of data protection law, particularly in relation to maintained schools.

- The DPO will report to the highest level of management.
- The DPO will operate independently and will not be dismissed or penalised for performing their task.
- Sufficient resources will be provided to the DPO to enable them to meet their UK GDPR and Data Protection Act 2018 obligations.
- The DPO will work alongside safeguarding leads to ensure that pupil/student data is protected as required.

The **Chief Privacy Officer (CPO)** is a key member of the school's senior management team and plays an important role in protecting the privacy of the school's students, staff, and visitors. They are also referred to as the **Data Protection Contact** or **Champion.** In this school this is the School Business Manager.

The CPO works closely with the DPO overseeing the school's data protection compliance which the data controller is ultimately responsible/accountable for. The DPO will assist the Data Controller to inform and advise the school and its employees about their obligations to comply with the UK GDPR and other data protection laws, monitor our compliance with the UK GDPR and other laws, including managing internal data protection activities, advising on data protection impact assessments, conducting internal audits, and providing the required training to staff members.

Lawful Processing

A record of processing activities is an efficient means of capturing all the important information about your school's data processing activities. It will improve your information governance and show your compliance with accountability principles. It will also ensure you comply with other aspects of data protection law, such as the requirement to create privacy notices and keep data assets secure, thereby reducing the risk of a personal data breach. At Hillcross Primary School we use a system called GDPRis.

The legal basis for processing data will be identified and documented prior to data being processed. Under the UK GDPR, data will be lawfully processed under one of the following conditions (Article 6):

a) Consent of the data subject
b) Processing is necessary for the performance of a contract with the data subject or to take steps to enter into a contract
c) Processing is necessary for compliance with a legal obligation
d) Processing is necessary to protect the vital interests of a data subject or another person
e) Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller

Necessary for the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject

In order to lawfully process special category data, we will identify both a lawful basis under Article 6 above and a separate condition for processing special category data under Article 9 below:

a) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject;
b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;
c) processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;
d) processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;
e) processing relates to personal data which are manifestly made public by the data subject;
f) processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;
g) processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;
h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;
i) processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for

suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;

j) processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

Consent

When we use consent as a legal basis for processing data, consent must be a positive indication. It cannot be inferred from silence, inactivity or pre-ticked boxes. Consent will only be accepted where it is freely given, specific, informed and an unambiguous indication of the individual's wishes.

Where consent is given, a record will be kept documenting how and when consent was given. We will ensure that consent mechanisms meet the standards of the UK GDPR. Where the standard of consent cannot be met, an alternative legal basis for processing the data must be found, or the processing must cease.

Consent accepted under the DPA will be reviewed to ensure it meets the standards of the UK GDPR; however, acceptable consent obtained under the DPA will not be reobtained. Consent can be withdrawn by a data subject at any time.

Data subjects' rights

Data subjects' rights over the use of their personal data are key to a privacy notice.

The Right to be informed -Privacy Notices

Privacy notices are the most common way of complying with data subjects' right to be informed. Under UK GDPR and the Data Protection Act 2018, every school has to make its privacy notices freely available to those whose personal data it handles. A privacy notice explains:

- why a school needs to collect personal data
- what it plans to do with it
- how long it will keep it
- whether it will be sharing it with any other organisation

Children have the same rights over their personal data as adults. We have a child-friendly privacy rights policy. We introduce the idea of data privacy within wider online safety lessons that allow teachers to use age-appropriate language, ensure understanding and encourage pupils to ask questions.

Our Privacy notices are clear and accessible on our school website, and regularly reviewed/updated. Being transparent builds trust, avoids confusion and lets everyone in the school community know what to expect.

The privacy notice supplied to individuals in regards to the processing of their personal data will be written in clear, plain language which is concise, transparent, easily accessible and free of charge. If services are offered directly to a child, we will ensure that the privacy notice is written in a clear, plain manner that the child will understand. In relation to data obtained both directly from the data subject and not obtained directly from the data subject, the following information will be supplied within our privacy notice:

a) the identity and the contact details of the controller and, where applicable, of the controller's representative;
b) the contact details of the data protection officer;
c) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;
d) the legitimate interests pursued by the controller or by a third party;
e) the recipients or categories of recipients of the personal data, if any;
f) where applicable, the fact that the controller intends to transfer personal data to a third country or international organisation with reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available.
g) the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;
h) the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability;
i) where the processing is based on point (a) of Article 6(1) or point (a) of Article 9(2), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;
j) the right to lodge a complaint with a supervisory authority;
k) whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data;
l) the existence of automated decision-making, including profiling and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

The Right of Access - Information Rights and SARs

Individuals have the right to obtain confirmation that their data is being processed.

Information rights mean a person has the right to access or amend the personal data any organisation, such as a school, holds about them. The most common type of information rights request is a subject access request (SAR). This is when someone requests to see the personal data an organisation holds about them. There is more information on to how to handle a SAR in a school and below.

Individuals, including children, have several information rights relating to personal data a school may hold about them. Information rights request that someone might make include asking to:

- change inaccurate personal information you hold about them
- remove their personal information or record
- restrict the processing of their personal information
- stop processing their personal information (right to object)

You can receive an information rights request relating to personal data either verbally or in writing, including through social media. Unless there is a valid reason, you must respond to any information rights request within one calendar month. If the case is complex you can extend the response deadline by an extra 2 calendar months. Information rights requests only apply to the personal data you hold when you get the request.

Individuals have the right to request changes or restrictions to personal information, but a school is not obliged to make changes to data in certain circumstances.

Subject Access Request (SAR)

Individuals have the right to submit a subject access request (SAR) to gain access to their personal data in order to verify the lawfulness of the processing. The school will refer to the DfE guidance referenced above when dealing with a SAR.

A requester can ask for any personal data that relates to:

- themselves
- someone they have parental responsibility for
- someone they have permission to act on behalf of

Requesting a SAR is a child's right. A child can request access to information about themselves from any education setting that holds data about them. A child does not have to be a certain age to make a SAR. The Information Commissioner's Office (ICO) provides guidance on the rights of children when making SARs. If the young person is under 13 and is making their own request, we will consider whether they will be able to understand your response, but this shouldn't be a barrier to supplying them with their information.

Where a SAR has been made for information held about a child, the school will evaluate whether the child is capable of fully understanding their rights. If the school determines the child can understand their rights, it will respond directly to the child.

We will verify the identity of the person making the request before any information is supplied.

In the event that a large quantity of information is being processed about an individual, you cannot ask the requester to narrow or reduce their request. You can ask for clarification of what specific information the requester is looking for. This might be helpful when the requester asks for a lot of information because they are not sure what they need. If the requester already has access to the information they want to see, you can direct them to this.

Schools can refuse to comply with a SAR if:

- a data protection exemption can be applied to all the personal information in scope of the request
- the request is manifestly unfounded or manifestly excessive

Examples of exemptions that may apply to education settings include:

- releasing the information would cause serious harm to a child
- releasing information would not be in the best interests of a child
- information relating to third parties
- legal advice sought and received from a lawyer
- information that may prejudice an investigation

A copy of the information will be supplied to the individual free of charge; however, we may impose a 'reasonable fee' to comply with requests for further copies of the same information. Where a SAR has been made electronically, the information will be provided in a commonly used electronic format. Where a request is manifestly unfounded, excessive or repetitive, a reasonable fee will be charged. All fees will be based on the administrative cost of providing the information.

All requests will be responded to without delay and at the latest, within one month of receipt. We will extend the SAR deadline if you have to wait for the requester to provide identification, authority and any clarification you might need. In the event of numerous or complex requests, the period of compliance will be extended by a further two months. The individual will be informed of this extension, and will receive an explanation of why the extension is necessary, within one month of the receipt of the request.

Where a request is manifestly unfounded or excessive, we hold the right to refuse to respond to the request. The individual will be informed of this decision and the reasoning behind it, as well as their right to complain to the supervisory authority and to a judicial remedy, within one month of the refusal.

The Right to Rectification

Individuals are entitled to have any inaccurate or incomplete personal data rectified. Where the personal data in question has been disclosed to third parties, we will inform them of the rectification where possible. Where appropriate, we will inform the individual about the third parties that the data has been disclosed to.

Requests for rectification will be responded to within one month; this will be extended by two months where the request for rectification is complex. Where no action is being taken in response to a request for rectification, we will explain the reason for this to the individual, and will inform them of their right to complain to the supervisory authority and to a judicial remedy.

The Right to Erasure

Individuals hold the right to request the deletion or removal of personal data where there is no compelling reason for its continued processing. Individuals have the right to erasure in the following circumstances:

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed
- When the individual withdraws their consent
- When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing
- The personal data was unlawfully processed
- The personal data is required to be erased in order to comply with a legal obligation
- The personal data is processed in relation to the offer of information society services to a child

We have the right to refuse a request for erasure where the personal data is being processed for the following reasons:

- To exercise the right of freedom of expression and information.
- To comply with a legal obligation for the performance of a public interest task or exercise of official authority
- For public health purposes in the public interest
- For archiving purposes in the public interest, scientific research, historical research or • statistical purposes
- The exercise or defence of legal claims

As a child may not fully understand the risks involved in the processing of data when consent is obtained, special attention will be given to existing situations where a child has given consent to processing and they later request erasure of the data, regardless of age at the time of the request.

Where personal data has been disclosed to third parties, they will be informed about the erasure of the personal data, unless it is impossible or involves disproportionate effort to do so.

Where personal data has been made public within an online environment, we will inform other organisations who process the personal data to erase links to and copies of the personal data in question.

The Right to Restrict Processing

Individuals have the right to block or suppress our processing of personal data. In the event that processing is restricted, we will store the personal data, but not further process it, guaranteeing that just enough information about the individual has been retained to ensure that the restriction is respected in future.

We will restrict the processing of personal data in the following circumstances:

- Where an individual contests the accuracy of the personal data, processing will be restricted until we have verified the accuracy of the data.
- Where an individual has objected to the processing and we are considering whether their legitimate grounds override those of the individual.
- Where processing is unlawful and the individual opposes erasure and requests restriction Instead.
- Where we no longer need the personal data but the individual requires the data to establish, exercise or defend a legal claim.

If the personal data in question has been disclosed to third parties, we will inform them about the restriction on the processing of the personal data, unless it is impossible or involves disproportionate effort to do so. We will inform individuals when a restriction on processing has been lifted.

The Right to Data Portability

Individuals have the right to obtain and reuse their personal data for their own purposes across different services. Personal data can be easily moved, copied or transferred from one IT environment to another in a safe and secure manner, without hindrance to usability.

The right to data portability only applies in the following cases:

- To personal data that an individual has provided to a controller
- Where the processing is based on the individual's consent or for the performance of a Contract
- When processing is carried out by automated means

Personal data will be provided in a structured, commonly used and machine-readable form. We will provide the information free of charge.

Where feasible, data will be transmitted directly to another organisation at the request of the individual. We use School 2 School (S2S), provided by the Department for Education, to securely transfer pupil records to and from other schools in a machine readable format.

- S2S is a secure data transfer website available to schools and Local Authorities in England and Wales.

- S2S has been developed to enable all data files required by DfE or by Local Authorities on behalf of DfE or which schools need to send to each other to be sent securely.

This school is not required to adopt or maintain processing systems which are technically compatible with other organisations.

In the event that the personal data concerns more than one individual, we will consider whether providing the information would prejudice the rights of any other individual.

We will respond to any requests for portability within one month.

The Right to Object

We will inform individuals of their right to object at the first point of communication, and this information will be outlined in the privacy notice and explicitly brought to the attention of the data subject, ensuring that it is presented clearly and separately from any other information. Individuals have the right to object to the following:

- Processing based on legitimate interests or the performance of a task in the public interest
- Direct marketing
- Processing for purposes of scientific or historical research and statistics.
- Where personal data is processed for the performance of a legal task or legitimate interests
- An individual's grounds for objecting must relate to his or her particular situation.
- We will stop processing the individual's personal data unless the processing is for the establishment, exercise or defence of legal claims, or, where we can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual.

Where personal data is processed for direct marketing purposes:

- We will stop processing personal data for direct marketing purposes as soon as an objection is received.
- We cannot refuse an individual's objection regarding data that is being processed for direct marketing purposes.

Where personal data is processed for research purposes:

- The individual must have grounds relating to their particular situation in order to exercise their right to object.

Where the processing of personal data is necessary for the performance of a public interest task, we are not required to comply with an objection to the processing of the data.

Where the processing activity is outlined above, but is carried out online, we will offer a method for individuals to object online.

Where the request is complex, or a number of requests have been received, the time frame can be extended by two months, ensuring that the individual is informed of the extension and the reasoning behind it within one month of the receipt of the request.

Where no action is being taken in response to a request, we will, without delay and at the latest within one month, explain to the individual the reason for this and will inform them of their right to complain to the supervisory authority and to a judicial remedy.

Data Protection by design and privacy impact assessments

We will act in accordance with the UK GDPR and Data Protection Act 2018 by adopting data protection by design approach and implementing technical and organisational measures which demonstrate how we have considered and integrated data protection into processing activities.

Data protection impact assessments (DPIAs) will be used to identify the most effective method of complying with our data protection obligations and meeting individuals' expectations of privacy. A DPIA is a tool to help you identify, measure and manage data protection risks. Under UK GDPR, a DPIA is needed whenever the processing of personal data is likely to result in a 'high risk to the rights and freedoms' of individuals.

We use a DPIA to:

- identify, manage and mitigate data protection risks
- fix problems at an early stage, minimising those risks
- consider and mitigate risks to individuals' privacy
- ensure individuals' expectations of privacy obligations are being met - for example, by the provision of privacy notices
- provide individuals with reassurance
- demonstrate both accountability and compliance with data protection law
- avoid reputational damage to your school

We carry out a DPIA of personal data collected:

- about vulnerable data subjects, including:
    - children (because of their age)
    - employees (because the power imbalance means they cannot easily consent or object to the processing of their data by an employer)
    - more vulnerable sectors of the population (who need special protection)
- by innovative technologies, such as:
    - biometrics
    - internet of things applications
    - safeguarding equipment, such as CCTV

DPIAs will allow us to identify and resolve problems at an early stage, thus reducing associated costs and preventing damage from being caused to this school's reputation which might otherwise occur. A DPIA will be used when using new technologies or when the processing is likely to result in a high risk to the rights and freedoms of individuals. A DPIA will be used for more than one project, where necessary.

High risk processing includes, but is not limited to, the following:

- Systematic and extensive processing activities, such as profiling

- Large scale processing of special categories of data or personal data which is in relation to criminal convictions or offences

We will ensure that all DPIAs include the following information:

- A description of the processing operations and the purposes
- An assessment of the necessity and proportionality of the processing in relation to the purpose · An outline of the risks to individuals
- The measures implemented in order to address risk
- Where a DPIA indicates high risk data processing, we will consult the ICO to seek its opinion as to whether the processing operation complies with the UK GDPR.

Data Breaches

The UK GDPR identifies personal data breaches as follows:

- "Confidentiality breach" - where there is an unauthorised or accidental disclosure of, or access to, personal data.
- "Availability breach" - where there is an accidental or unauthorised loss of access to, or destruction of, personal data.
- "Integrity breach" - where there is an unauthorised or accidental alteration of personal data.

The Senior Leadership Team will ensure that all staff members are made aware of, and understand, what constitutes a data breach as part of their continuous development training.

Where a breach is likely to result in a risk to the rights and freedoms of individuals, the relevant supervisory authority will be informed.

All notifiable breaches will be reported to the relevant supervisory authority within 72 hours of us becoming aware of it.

The risk of the breach having a detrimental effect on the individual, and the need to notify the relevant supervisory authority, will be assessed on a case-by-case basis.

In the event that a breach is likely to result in a high risk to the rights and freedoms of an individual, we will notify those concerned directly.

A 'high risk' breach means that the threshold for notifying the individual is higher than that for notifying the relevant supervisory authority.

In the event that a breach is sufficiently serious, the public will be notified without undue delay.

Effective and robust breach detection, investigation and internal reporting procedures are in place which facilitate decision-making in relation to whether the relevant supervisory authority or the public need to be notified.

Within a breach notification, the following information will be outlined:

- The nature of the personal data breach, including the categories and approximate number of individuals and records concerned

- The name and contact details of the DPO
- An explanation of the likely consequences of the personal data breach
- A description of the proposed measures to be taken to deal with the personal data breach
- Where appropriate, a description of the measures taken to mitigate any possible adverse effects

Failure to report a breach when required to do so may result in action by the Information Commissioner.

The school will ensure all facts regarding the breach, the effects of the breach and any decision-making processes and actions taken are documented in line with UK GDPR and Data Protection Act 2018 accountability principle and in accordance with the Records Management Policy.

The school will work to identify the cause of the breach and assess how a recurrence can be prevented e.g. by mandating data protection refresher training where the breach was a result of human error.

Data Security

- Confidential paper records will be kept in a locked filing cabinet, drawer or safe, with restricted access.
- Confidential paper records will not be left unattended or in clear view anywhere with general access.
- Visitors to areas containing sensitive information are supervised at all times.

- Digital data is coded, encrypted or password-protected, both on a local hard drive and on a network drive that is regularly backed up off-site. This school uses the LGFL Gridstore System for off-site backup.

- Where data is saved on removable storage or a portable device, this device will be encrypted using Advanced Encryption Standard (AES) 256-Bit Security to FIPS-197 standard. Such devices will be kept in a locked filing cabinet, drawer or safe when not in use. E.g. memory sticks will not be used to hold personal information unless they are password-protected and fully encrypted and all electronic devices are password-protected to protect the information on the device in case of theft.

- Where possible, we enable electronic devices to allow the remote blocking or deletion of data in case of theft or loss.
    - Staff and governors will not use their personal laptops, computers or other devices for school business without prior permission of the headteacher - where this is the case this is declared and a record kept. If permission is given, all documents will be saved securely and deleted as soon as they are no longer needed.
    - Staff and governors can access Google Drive from a personal machine as long as documents are not saved to it.
    - Staff and governors will not use personal email accounts or personal cloud storage for school business.
    - To aid with operational efficiency, the leadership team and school governors can set up their personal (not shared family) devices such as their phone or tablet to automatically access their school email account as long as this is password protected.
    - All other staff can only access their school email account by logging in via the internet. When staff are using their own devices it is strongly recommended that they access their email account using Microsoft Outlook web access (OWA) This ensures data is kept on the server and not downloaded onto the device.

- Members of staff who access the school network are provided with their own secure login and password, and every computer regularly prompts users to change their password. Access to files on the school network is on a need to know basis - files and folders have granular permissions based on staff seniority and role. File access is monitored and reviewed.

- Remote access to school systems is permitted based on a credible business case. When permission is granted remote access will be via LGFL CISCO AnyConnect Use of second factor authentication is mandatory for remote access to the school network. This includes the use of both 'soft' and 'hard' One Time Passwords.

- Wi-Fi access to the school network is permitted from school devices. Staff owned devices and visitors must use the separate Guest Wi-Fi.

- Email is not a secure medium for external communication and should be used as a last resort for sending sensitive or confidential information. If documents are sent by email they should be encrypted with a password. This school uses the Secure Document Transfer Portal (USO-FX) provided by the LGFL to transfer information securely. Circular emails to parents are sent blind carbon copy (bcc), so email addresses are not disclosed to other recipients.

- Where personal information that could be considered private or confidential is taken off the premises, either in electronic or paper format, staff will take extra care to follow the same procedures for security, e.g. keeping devices under lock and key. The School Business Manager, Designated Safeguarding Leads and the SENDCO have lockable security pouches to minimise the risk of a data breach should data sensitive documentation need to be taken off site. The person taking the information from school premises accepts full responsibility for the security of the data.

Before sharing data, all staff members will ensure:

- They are allowed to share it.
- That adequate security is in place to protect it.
- Who will receive the data has been outlined in a privacy notice.

The physical security of our buildings and storage systems, and access to them, is reviewed on a termly basis. If an increased risk in vandalism/burglary/theft is identified, extra measures to secure data storage will be put in place. This school takes its duties under the UK GDPR and Data Protection Act 2018 seriously and any unauthorised disclosure may result in disciplinary action.

The Data Protection Officer will assist in making sure that continuity and recovery measures are in place to ensure the security of protected data.

Where Data is taken off site: Educational visits

Staff will ensure all risk assessments and other data sensitive documentation are managed securely on the day of the visit.

- When not being referred to, all documentation such as risk assessments should be kept securely in staff members bags during the visit to prevent a potential data breach.
- Different documentation should be kept separately in plastic wallets to minimise a breach in data should any document be mislaid e.g. risk assessments, tickets, maps, groupings.

- Any pupil sensitive information given to parents/visitors supporting the school visit should be on a 'need to know' basis only e.g. only the medical conditions of the children in their group should be shared.
- All documentation given to additional adults should be collected back at the end of the visit by the party leader.

Safeguarding

The school understands that the UK GDPR and Data Protection Act 2018 does not prevent or limit the sharing of information for the purposes of keeping children safe.

The school will ensure that information pertinent to identify, assess and respond to risks or concerns about the safety of a child is shared with the relevant individuals or agencies proactively and as soon as is responsibly possible.

Where there is doubt over whether safeguarding information is to be shared, especially with other agencies, the DSL will ensure that they record the following information:

- Whether the data was shared
- What data was shared
- With whom data was shared
- For what reason data was shared
- Where a decision has been made not to seek consent from the data subject or their parent
- The reason that consent that consent has not been sought, where appropriate

The school will aim to gain consent to share information where appropriate; however, will not endeavour to gain consent if to do so would place a child at risk.

Publication of Information

This school publishes a publication scheme on its website outlining classes of information that will be made routinely available, including:

- Policies and procedures
- Annual reports
- Financial information

Classes of information specified in the publication scheme are made available quickly and easily on request. This school will not publish any personal information, including photos, on its website without the permission of the affected individual.

When uploading information to the website, staff are considerate of any metadata or deletions which could be accessed in documents and images on the site.

CCTV and Photography

We understand that recording images of identifiable individuals constitutes processing personal information, so it is done in line with data protection principles.

We notify all pupils, staff and visitors of the purpose for collecting CCTV images via notice boards, letters and email.

Cameras are only placed where they do not intrude on anyone's privacy and are necessary to fulfil their purpose. All CCTV footage will be kept for six months for security purposes; the Data Protection Officer is responsible for keeping the records secure and allowing access.

We will always indicate our intentions for taking photographs of pupils and will retrieve permission before publishing them.

If we wish to use images/video footage of pupils in a publication, such as our website, prospectus, or recordings of school plays, written permission will be sought for the particular usage from the parent of the pupil.

Images captured by individuals for recreational/personal purposes, and videos made by parents for family use, are exempt from the UK GDPR and Data Protection Act 2018.

Data Retention

Data will not be kept for longer than is necessary. We document all information we hold and dispose of data according to our retention schedule.

The Department for Education recognises that further guidance is required in this area and we will incorporate any new standard approach into our record management practice as it emerges. [1]

Unrequired data will be deleted as soon as practicable.

Some educational records relating to former pupils or employees may be kept for an extended period for legal reasons, but also to enable the provision of references or academic transcripts.

Paper documents will be cross cut shredded or pulped, and electronic memories scrubbed clean or destroyed, once the data should no longer be retained.

A certificate of destruction will be obtained when computer hard drives that have held personal information are disposed of.

DBS Data

- All data provided by the DBS will be handled in line with data protection legislation; this includes electronic communication.
- Data provided by the DBS will never be duplicated.
- Any third parties who access DBS information will be made aware of the data protection legislation, as well as their responsibilities as a data handler.

Definitions

Definitions used by this school (drawn from the UK GDPR)

[1] "work will be done to develop a consistent voice that supports schools by generating and sharing exemplar data retention policy." DFE "Data Protection a toolkit for Schools" April 2018

Material scope (Article 2) – the UK GDPR applies to the processing of personal data wholly or partly by automated means (i.e. by computer) and to the processing other than by automated means of personal data (i.e. paper records) that form part of a filing system or are intended to form part of a filing system.

Territorial scope (Article 3) – the UK GDPR and Data Protection Act 2018 will apply to all controllers that are established in the EU (European Union) who process the personal data of data subjects, in the context of that establishment. It will also apply to controllers outside of the EU that process personal data in order to offer goods and services, or monitor the behaviour of data subjects who are resident in the EU.

Article 4 definitions

Establishment – the main establishment of the controller in the EU will be the place in which the controller makes the main decisions as to the purpose and means of its data processing activities. The main establishment of a processor in the EU will be its administrative centre. If a controller is based outside the EU, it will have to appoint a representative in the jurisdiction in which the controller operates to act on behalf of the controller and deal with supervisory authorities.

Personal data – any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Special categories of personal data – personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

Data controller – the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

Data subject – any living individual who is the subject of personal data held by an organisation.

Processing – any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Profiling – is any form of automated processing of personal data intended to evaluate certain personal aspects relating to a natural person, or to analyse or predict that person's performance at work, economic situation, location, health, personal preferences, reliability, or behaviour. This definition is linked to the right of the data subject to object to profiling and a right to be informed about the existence of profiling, of measures based on profiling and the envisaged effects of profiling on the individual.

Personal data breach – a breach of security leading to the accidental, or unlawful, destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed. There is an obligation on the controller to report personal data breaches to the supervisory authority and where the breach is likely to adversely affect the personal data or privacy of the data subject.

Data subject consent - means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data.

Child – the UK GDPR and Data Protection Act 2018 defines a child as anyone under the age of 16 years old, although this may be lowered to 13 by Member State law. The processing of personal data of a child is only lawful if parental or custodian consent has been obtained. The controller shall make reasonable efforts to verify in such cases that consent is given or authorised by the holder of parental responsibility over the child.

Third party – a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data.

Filing system – any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis. **Data Protection Officer** (DPO) – person responsible for informing and advising an organisation about their data protection obligations, and monitoring their compliance with them.

Chief Privacy Officer (CPO) – person responsible for implementing and developing data protection as communicated by the DPO.

Equality Impact Assessment

Under the Equality Act 2010 we have a duty not to discriminate against people on the basis of their age, disability, gender, gender identity, pregnancy or maternity, race, religion or belief and sexual orientation. We are committed to treating all members of the school community fairly and challenging negative attitudes about disability and accessibility and to developing a culture of awareness, tolerance and inclusion. This policy has been equality impact assessed and we believe that it is in line with the Equality Act 2010 as it is fair, it does not prioritise or disadvantage any member of the school community and it helps to promote equality and accessibility at our school. The curriculum is planned to be inclusive and meet the needs and interests of a full range of learners. Activities and resources will be differentiated and adult support used to ensure that children access the curriculum and make the best possible progress.

Safeguarding Commitment

The school is committed to safeguarding and promoting the welfare of children, in line with the most recent version of Keeping Children Safe in Education, and expects all staff and volunteers to share this commitment. We take seriously our duty of care to our pupils and staff which includes safeguarding them from the risk of being drawn into terrorism - this includes not just violent extremism but also non-violent extremism, which can create an atmosphere conducive to terrorism and can popularise views which terrorists exploit. We work closely with social care, the police, health services and other services to promote the welfare of children and protect them from harm. Radicalisation is recognised as a specific safeguarding issue and is addressed in line with the Government Prevent Strategy and The Counter-Terrorism and Security Act 2015.

Privacy Policy

Hillcross School is committed to ensuring protection of all personal information that we hold. We recognise our obligations under the GDPR and Data Protection act 2018. Our practice is documented in our Data Protection Policy.

Hillcross Primary School

Monitoring and Evaluation

Review Cycle: This policy will be reviewed annually or earlier in the light of experience, or because of operational or organisational changes or for any other reason that the policy ceases to be valid.

Reviewed : **June 2024**
Date of next review : June 2025