Crosby Primary School

Data Protection Policy

2021-2024

CONTENTS

Introduction to Data Protection 4

Purpose 4

Key Definitions 5

Personal and Sensitive Data 6

Data Protection Principles 7

The Data Controller 7

Information Sharing, Access and Disclosure 8

Sharing Personal Information 8

Requests for Information in the Education Record 9

Pupil Information Regulations 9

Parental Requests to see the Educational Record 9

Data Protection Section 29 and Section 35 Requests for Information 10

Freedom of Information Request for Information 10

Environmental Information Regulation Requests for Information 11

Re-use of Information 12

Publication Scheme 12

Closed Circuit Television (CCTV) 13

Photographs and Videos 13

Roles and Responsibilities 13

All Staff 13

Technical Compliance 14

Governing body 14

Data Protection Officer 14

Headteacher 14

School Business Manager 15

Data Protection by Design and Default 15

Data Protection Impact Assessments 16

Records Management 16

Data Security and Storage of Records 16

Inventory of Records and Retention Schedule 17

What is a Record? 17

Management of electronic and/or email records 17

Records Management Lifecycle 17

Record maintenance and storage 18

Retention and disposal 19

Security Incidents and Data Breaches 19

Data Breaches 20

Training 22

Complaints 22

How to appeal against the outcome of an Information Complaint 22

Links with other policies and procedures 22

Monitoring arrangements 22

Appendix 1: Legislation 23

Appendix 2: Exemptions and Exceptions 24

Appendix 3: Information Request Charging 27

Appendix 4: Information Sharing Statement 29

Introduction to Data Protection

Information stored and processed by the school is a valuable asset. It is vital that the best use is made of this asset to inform decision making, improve accountability, and enhance services. Crosby Primary School is committed to upholding the data protection principles and the protection of all personal and sensitive information/special category data collected about staff, pupils, parents, governors, job applicants, visitors, contractors and any other individuals.

We ensure that all personal and sensitive data is collected, stored and processed in accordance with the principles of the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA 2018).

Without adequate levels of protection, confidentiality, integrity and availability the school will not be able to fulfil its obligations including the provision of education and meeting legal and statutory requirements such as being able to respond to requests for information in a timely fashion.

We monitor and implement any changes to data protection legislation to remain compliant. The school must comply with legislation to function efficiently. Further details of relevant legislation can be found in Appendix 1.

This policy sets out how we will comply with these principles by providing the framework through which this effective management can be achieved and audited.

Purpose

The purpose of this policy is to ensure that data is managed appropriately. It sets out the school's commitment to data protection and provides the controls and requirements that will protect the wide range of information held or processed by the school, and ensuring all forms of information, supporting systems and networks are protected from security threats.

The key objectives are to:

- protect the school's information from all threats whether internal or external, deliberate or accidental;
- build an information management culture where records are managed consistently, in a safe and secure environment, and with appropriate level of:
    - **Confidentiality:** to prevent unauthorised disclosure of information
    - **Integrity**: to prevent the unauthorised amendment or deletion of information
    - **Availability:** to prevent the non-availability of information and the unauthorised withholding of it.
- ensure compliance with legislation and standards;
- manage records so that they can properly support the school's objectives;
- make best use of physical and electronic storage space;
- ensure information is accessible when appropriate and required;
- ensure records are kept for no longer than is necessary and are disposed of or retained correctly;
- ensure the school's vital records are identified and protected (i.e. those required to maintain business continuity in the event of a disaster, and without which the school could not operate);
- make best use of employee time;
- ensure employees receive appropriate training.

Key Definitions

Term	Definition
Personal information	Any information relating to an identified, or identifiable natural person (data subject). This may include the individual's: • Name (including initials) • Identification number • Location data • Online identifier, such as a username It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity. Personal information can be factual (for example, a name, email address, location or date of birth) or an opinion about that person's actions or behaviour.
Sensitive or Special categories of personal information	Personal information which is more sensitive and so needs more protection, including information about an individual's: • Racial or ethnic origin • Political opinions • Religious or philosophical beliefs • Trade union membership • Genetics • Health – physical or mental • Sex life or sexual orientation • Criminal offences and convictions
Processing	Anything done to personal information, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disclosing, disseminating or otherwise making available, restricting, erasing or destroying. Processing can be automated or manual.
Data subject	A living, identified or identifiable individual about whom we hold or process personal information. Data subjects may be nationals or residents of any country and may have legal rights regarding their personal information.
Data controller	A person or organisation that determines the purposes and the means of processing of personal information. It is responsible for establishing practices and policies in line with the UK GDPR. The school is the Data Controller of all personal information relating to its pupils, parents and staff.
Data processor	A person or other body, other than an employee of the data controller, who processes personal information on behalf of the data controller.
Data Protection Officer (DPO)	The person required to be appointed in public authorities under the UK GDPR. In this school our DPO is Tim Pinto tpinto@esafetyoffice.co.uk

Term	Definition
Data breach (Personal data breach)	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal information.
Privacy by design	Implementing appropriate technical and organisational measures in an effective manner to ensure compliance with the UK GDPR.
Data Protection Impact Assessment (DPIA)	Tools and assessments used to identify and reduce risks of a data processing activity. DPIA can be carried out as part of Privacy by Design and should be conducted for all major systems or business change programs involving the processing of personal information.
Privacy Notices	Separate notices setting out information that may be provided to data subjects when the school collects information about them. These notices may take the form of general privacy statements applicable to a specific group of individuals (for example, school workforce privacy policy) or they may be stand-alone privacy statements covering processing related to a specific purpose.
Consent	Agreement which must be freely given, specific, informed and be an unambiguous indication of the data subject's wishes by which they, by a statement or by a clear positive action, signify agreement to the processing of personal information relating to them.

Personal and Sensitive Data

For the purpose of this policy, personal data refers to that which relates to an identifiable, living individual, including information such as an online identifier, such as an IP address.

The UK GDPR applies to both automated personal data and to manual filing systems. This policy applies to all personal data, regardless of whether it is in paper or electronic format and references to 'data' or 'information' apply to both.

Sensitive data is also referred to as 'special category data'. The UK GDPR defines special category data as:

- personal data revealing racial or ethnic origin;
- personal data revealing political opinions;
- personal data revealing religious or philosophical beliefs;
- personal data revealing trade union membership;
- genetic data;
- biometric data (where used for identification purposes);
- data concerning health;
- data concerning a person's sex life; and
- data concerning a person's sexual orientation.

This does not include personal data about criminal allegations, proceedings or convictions, as separate rules apply.

Data Protection Principles

Article 5 of the UK GDPR sets out seven key principles which lie at the heart of the general data protection regime. Article 5(1) requires that personal data shall be:

(a) processed lawfully, fairly and in a transparent manner in relation to individuals ('l**awfulness, fairness and transparency**');

(b) 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 ('**purpose limitation**');

(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('**data minimisation**');

(d) 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 ('**accuracy**');

(e) 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 GDPR in order to safeguard the rights and freedoms of individuals ('**storage limitation**');

(f) 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 ('**integrity and confidentiality**').

Article 5(2) adds that:

- The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('**accountability**').

The Data Controller

Crosby Primary School processes personal information relating to parents, pupils, staff, governors, visitors and others, and therefore is the data controller.

The school is registered as a data controller with the ICO under reference Z5354604 and will renew this registration annually or as otherwise legally required.

Data Protection Rights of the Individual

The UK GDPR provides the following rights for individuals:

1. The right to be informed
2. The right of access
3. The right to rectification
4. The right to erasure
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights in relation to automated decision making and profiling.

Individuals have the right to:

- Withdraw their consent to processing at any time

- Ask us to rectify, erase or restrict processing of their personal information, or object to the processing of it (in certain circumstances)
- Prevent use of their personal information for direct marketing
- Challenge processing which has been justified on the basis of public interest
- Request a copy of agreements under which their personal information is transferred outside of the European Economic Area
- Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them)
- Prevent processing that is likely to cause damage or distress
- Be notified of a data breach in certain circumstances
- Make a complaint to the ICO
- Ask for their personal information to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)

Individuals should submit any request to exercise these rights to the DPO. If staff receive such a request, they must immediately forward it to the DPO.

Information Sharing, Access and Disclosure

Personal and confidential information will be shared within the school and with other organisations in line with the law and where there is a need or obligation to do so. Where there is a need to share information with external organisations the information sharing will be governed either under the terms of a contract and / or an information sharing or information access / disclosure agreement.

Education Records held within the school MIS are transferred using the DFE secure transfer service. Safeguarding records held within the CPOMS system are transferred under the authority of the Headteacher. Where additional information is held this is sent electronically, under secure email, and recipient schools are asked to confirm that records have been received. In the event that records have to be sent by post, registered post or recorded delivery will be used to ensure they have been received. We ensure we include the information sharing agreement shown at Appendix 4 when we transfer records

We follow The Humber Information Sharing Charter and use the template within it to guide our data sharing agreements as necessary.

Sharing Personal Information

We will not normally share personal information with anyone else, but may do so where:

- there is an issue with a pupil or parent/carer that puts the safety of them or our staff at risk.
- we need to liaise with other agencies – we will seek consent if necessary before doing this.
- our suppliers or contractors need data to enable us to provide services to our staff and pupils – for example, IT companies. When doing this, we will:
    - only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law.
    - establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal information we share.
    - only share data that the supplier or contractor needs to carry out their service, or information necessary to keep them safe while working with us.

We will share personal information with law enforcement and government bodies where we are legally required to do so, including for:

- The prevention or detection of crime and/or fraud.
- The apprehension or prosecution of offenders.
- The assessment or collection of tax owed to HMRC.
- In connection with legal proceedings.

- Where the disclosure is required to satisfy our safeguarding obligations.
- Research and statistical purposes, as long as personal information is sufficiently anonymised or consent has been provided.

Requests for Information in the Education Record
Pupil Information Regulations
Maintained schools have a responsibility under the Pupil Information Regulations (PIR) to deal with requests for access to Education Record information. The PIR sets out a series of exemptions that allow all or some information from the Education Record to be withheld.

The Information Commissioner's Office (ICO) regulates this legislation in the UK and copies of their guidance notes can be accessed at www.ico.org.uk. We also have a Publication Scheme which sets out documents that are available.

Parental Requests to see the Educational Record
Parents, or those with parental responsibility, have a legal right to free access to their child's educational record (which includes most information about a pupil) within 15 school days of receipt of a written request. Requests for information in an Education Record can be made by someone with Parental Responsibility or a child who is mature enough to understand their rights and the child cannot prevent a response being sent to the parent.

Subject Access Requests (SAR)
Schools have a responsibility under the DPA to deal with individual requests for recorded personal information. These are known as Subject Access Requests or SARs and might be made for employee or pupil information.

Individuals have a right to make a subject access request to gain access to personal information that the school holds about them.

If staff receive a subject access request they must immediately forward it to the DPO.

In each case a legal timeframe must be complied with. The legal response time permitted varies depending on whether any part of the request is for the Education Record or other personal information. If the request is solely or partly for information in the Education Record the school will aim to respond within 15 school days. The aim for other requests will be 40 consecutive days.

Requests for information:
- Must be in writing to admin.crosbyprimary@northlincs.gov.uk or addressed to the school.
- Must provide the requester's real name and address and proof of identification.
- Must clearly describe the information being requested.
- Should ideally state the format the requester would like to receive the information in.
- Do not have to mention the words DPA, SAR or PIR in the request.

The school will acknowledge requests within 5 school days.

The timeframe starts on the next school or working day after the request is received. School days are any days when pupils are in attendance and working days are any day other than Saturday, Sunday, public holidays, bank holidays, school holidays and training days when pupils are not in attendance.

If the request genuinely cannot be understood, clarification will be sought promptly from the requester and the response time will not start until the request is understood and agreed.

Requests for information can be refused for reasons including:
- The information is not held.
- The request is for someone else's personal information or Education Record and the requester does not have consent or is not entitled to see it.

- A SAR request has been made for a child's information from someone with parental consent where the child is considered mature enough to make their own request and has not given consent for the requester to do so on their behalf. Children are generally considered mature enough to make their own request from 12 years of age.

Details about any charges that could apply are shown in Appendix 3. If a fee is due this will also be promptly requested and the response timeframe will be put on hold until payment is received.

If we are able to release the requested information we will collate it, advise that the information is held and provide a copy. The information provided will be in the format requested if this format is reasonably practicable. Sometimes we will need to redact information, if for example someone could be identified that should not be. If we are unable to provide some or all information we will explain why in writing within the permitted timeframe.

SAR requests can also be made by a third party with the permission of the person to whom the information relates. If a child is not considered mature enough generally an adult with parental responsibility could make the request on their behalf, but this is a case by case decision based on what is in the best interests of the child.

If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee which takes into account administrative costs. A request will be deemed to be unfounded or excessive if it is repetitive, or asks for further copies of the same information. When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO.

Advice and assistance to make a successful request can be obtained by contacting the Data Protection Officer tpinto@esafetyoffice.co.uk.

Data Protection Section 29 and Section 35 Requests for Information
DPA Section 29 and Section 35 requests for information will be considered on a case by case basis and on occasion a school will decide not to release information without a court order.

We may also share personal information with emergency services and local authorities to help them to respond to an emergency situation that affects any of our pupils or staff.

Where we transfer personal information to a country or territory outside the European Economic Area, we will do so in accordance with data protection law.

Freedom of Information Request for Information
Requests for information under the FOIA:

- Must be in writing.
- Must provide the requester's real name and a correspondence address.
- Must describe the information being requested.
- Should ideally state the format the requester would like to receive the information in.
- Do not have to mention the FOIA in the request.

Any request that cannot be answered promptly as part of normal day to day business or where the requester asks for it to be handled under FOIA will be treated as a potential FOIA request.

The school aims to acknowledge requests within 5 school days and respond to requests within 20 school days, or 60 working days if this is shorter. This timeframe starts on the next school or working day after the request is received. School days are any days when pupils are in attendance and working days are any day other than Saturday, Sunday, public holidays, bank holidays, school holidays and training days when pupils are not in attendance.

If the request genuinely cannot be understood clarification will be promptly sought from the requester and the response time will not start until the request is understood and agreed.

Requests for information under the FOIA can be refused for reasons including:

- The information is not held.
- It would cost too much or take up too much of someone's time.
- The request is considered vexatious.
- The request is considered repeated.

Information can also be withheld from a requester if one or more of the exemptions listed in the FOIA, as shown in Appendix 2 apply.

Details about the FOIA fee limit and how it is calculated and any other charges that may apply are shown as Appendix 3. If a fee is due this will also be promptly requested and the response timeframe will be put on hold until payment is received.

If we are able to release the requested information we will collate it, advise that the information is held and provide a copy in a format requested if this is reasonably practicable. Information will be redacted, if for example someone would be identified who should not be. If we are unable to provide some or all information we will explain why in writing within the permitted timeframe.

If the information being released is a dataset wherever possible we will provide it in a re-usable format. Datasets requested under FOIA will be made available via the Publication Scheme with regular updates, unless this is not practical.

Environmental Information Regulation Requests for Information

Schools have two main responsibilities under the EIR, as follows:

- To proactively publish environmental information in an accessible electronic format whenever possible
- Deal with individual requests for environmental information

Environmental Information Definition

a) The state of the elements of the environment – e.g. air, atmosphere, water, soil, land, landscape and natural sites such as wetlands, coastal and marine areas, biological diversity and the interaction of these elements;

b) Factors affecting (or likely to affect) the environment – including energy, noise, radiation, waste, emissions, discharges and other releases into the environment.

c) Measures – such as policies, legislation, plans, programmes, environmental agreements and activities affecting or likely to affect the elements and factors referred to above;

d) Reports – on the implementation of environmental legislation;

e) Economic analyses – including cost benefit and other economic analyses and assumptions used within the framework of measures and activities referred to in (c);

f) The state of human health and safety – including the contamination of the food chain, conditions of human life, cultural sites and built structures insofar as they are or may be affected by the state of the elements of the environment referred to in (a) or through those elements by any of the matters referred to in (b) or (c).

The EIR provides a right of access to both individuals and organisations to recorded environmental information held by a school. This includes paper records, emails, information stored on computer, audio records, photographs, handwritten notes or any other form of recorded information.

Information is considered to be held if it relates to the business of the school and has been created or received by the school or if it is being held by another organisation on the school's behalf.

The Code of Practice on the discharge of the obligations of public authorities under EIR sets out good practice recommendations for handling EIR requests.

Requests for information under the EIR:

- Can be verbal or in writing.
- Must provide a name and contact address.
- Must describe the information being requested.
- Should ideally state the format the requester would like to receive the information in.
- Does not have to mention the EIR in the request.

Any request that cannot be answered promptly as part of normal day to day business or where the requester asks for it to be handled under EIR will be treated as a potential EIR request.

The school aims to acknowledge requests within 5 school days and respond to requests within 20 working days but this can be extended to 40 working days for complex or voluminous requests. This timeframe starts on the next working day after the request is received. Working days are any day other than Saturday, Sunday, public holidays, bank holidays as set out by the Financial Dealings Act 1971.

If the request genuinely cannot be understood clarification will be promptly sought from the requester and the response time will not start until the request is understood and agreed.

Requests for information under the EIR can be refused for reasons including:

- The information is not held.
- The request is considered manifestly unreasonable.
- The request is considered repeated.

Information can also be withheld from a requester if one or more of the exceptions listed in the EIR and as shown in Appendix 2 applies.

Details about any charges that could apply are shown in Appendix 3. If a fee is due this will also be promptly requested and the response timeframe will be put on hold until payment is received.

If we are able to release the requested information we will collate it, advise that the information is held and provide a copy in the format requested if this is reasonably practicable. We will redact information, if for example someone would be identified who should not be. If we are unable to provide some or all information we will explain why in writing within the permitted timeframe.

If the information being released is a dataset wherever possible we will provide the dataset in a re-usable format. Datasets requested under EIR will be made available via the Publication Scheme with regular updates, unless this is not practical.

Re-use of Information

Anyone can ask to re-use information that has already been made accessible by a school. Requests should be made in writing and will be responded to within 20 working days, as set out by the Re-use of Public Sector Information Regulations 2015 (RPSI).

In the spirit of transparency information will be made available for re-use free of charge whenever possible.

Publication Scheme

The Model Publication Scheme for Schools, approved by the ICO, has been adopted. We are committed to publish certain information and to:

1. Make the Publication Scheme and the information in it available to the public.
2. Explain how information can be obtained and if there is a charge.
3. Publish any dataset that has been released in response to a request for information in a re-usable form.

4. Make any published datasets that are 'relevant copyright works' where the school is the only owner available for re-use under a specified licence, which may be chargeable, but if possible will be free under the Open Data Licence.
5. Routinely review and update all published information, including dataset information, unless in the case of datasets it is not appropriate to do so.

Closed Circuit Television (CCTV)
We use CCTV in various locations around the school site to ensure it remains safe. We will adhere to the ICO's code of practice for the use of CCTV.

We do not need to ask individuals' permission to use CCTV, but we make it clear where individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use.

Any enquiries about the CCTV system should be directed to the School Business Manager or Headteacher.

Photographs and Videos
As part of our school activities, we may take photographs and record images of individuals within our school.

We will obtain written consent from parents/carers for photographs and videos to be taken of their child for communication, marketing and promotional materials. We will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil.

Uses may include:

- Within school on notice boards and in school magazines, brochures, newsletters, etc.
- Outside of school by external agencies such as the school photographer, newspapers, campaigns
- Online on our school website or social media pages

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not distribute it further.

See our Online Safeguarding Policy and Acceptable Use of Information and Communication Technology Policy for more information on our use of photographs and videos.

It is the school's policy that external parties (including parents/carers) may not capture images of staff or pupils during school activities without prior consent from the Headteacher.

Roles and Responsibilities
All Staff
All staff have the responsibility to treat all information in a confidential manner and follow the guidance as outlined within this policy. The school is committed to ensuring that its staff are aware of data protection policies, legal requirements and adequate, regular training is provided.

This policy is in place to ensure all staff and governors are aware of their responsibilities in relation to the core principles of the UK GDPR and applies to all staff employed by our school, and to external organisations or individuals contracted to provide services within the school. Staff who do not comply with this policy may face disciplinary action.

Staff are responsible for:

- Collecting, storing and processing any personal information in accordance with this policy.
- Informing the school of any changes to their personal information, such as a change of address.
- Contacting the DPO in the following circumstances:
    - With any questions about the operation of this policy, data protection law, retaining personal information or keeping personal information secure.
    - If they have any concerns that this policy is not being followed.

- If they are unsure whether they have a lawful basis to use personal information in a particular way.
- If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal information outside the European Economic Area.
- If there has been a data breach.
- Whenever they are engaging in a new activity that may affect the privacy rights of individuals.
- If they need help with any contracts or sharing personal information with third parties.
- If staff receive a subject access request or freedom of information request.

To help protect people's personal information keep to these useful rules:

- Always treat people's personal information with integrity and confidentiality
- Read and understand the Acceptable Use of ICT policy
- Know what the data protection principles are and apply them
- Any new system or service that involves personal information requires a Data Protection Impact Assessment to be carried out *before* commencement
- Store hard copies securely and transfer them directly to recipients
- Use your encrypted USB drives to store and transfer data where needed
- You have an organisational email address with a 'my files' area. Use it rather than send data to your personal email
- Be alert to cyberattacks and report suspicious emails or calls
- Report losses of data or devices as soon as possible
- Take care to use the 'bcc' option for bulk emailing
- Beware of autocomplete on email - check you are sending to the right address
- Ensure any personal device has appropriate security measures if using it for work-related activity
- If you have a question about any data protection issue, ask the School Business Manager or the Data Protection Officer (DPO)

Technical Compliance

The ICT Infrastructure Officer will ensure that information systems are checked regularly to ensure they are still protected by the most up to date security available.

Governing body

The governing body has overall responsibility for ensuring that our school complies with all relevant data protection obligations. The governor responsible for Information Governance is Miss Jenny Harrison.

Data Protection Officer

The Data Protection Officer (DPO) is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable.

They provide an annual audit report and, where relevant, provide advice and recommendations on school data protection issues.

The DPO is also the first point of contact for individuals whose data the school processes, and for the ICO.

Our DPO is Mr Tim Pinto, he is contactable via email tpinto@esafetyoffice.co.uk.

Headteacher

The Headteacher, Mrs Heather Reid, acts as the representative of the data controller on a day-to-day basis.

The Headteacher and appointed deputy are responsible for the following:

- The Records Management process.
- Promoting compliance with this policy.
- Investigating non-compliance with this policy.

- Making decisions about and approving retention and disposal or transfer to permanent archive.

The Local Authority's Information Governance function may be asked to provide support as set out in the Services to School, Information and IT Security annual offer.

The Headteacher is the senior responsible member of staff for information security/risk and leads the school's response by:

- Fostering a culture for protecting and appropriately using information
- Providing a focal point for managing information risks and incidents
- Ensuring that all information assets and the records they contain are managed
- Ensuring that employees have the appropriate level of access to the information they need and are familiar and compliant with their responsibilities under the Data Protection Act 2018.
- Ensuring that risk assessments are carried out and appropriate controls implemented.
- Ensuring that actual or potential security incidents are recognised and appropriate action taken to stop the incident, investigate and make changes where necessary.
- Ensuring that contractors, partner organisations and third parties have appropriate and satisfactory systems and procedures in place and agreed terms and conditions consistent with this policy before doing business with the school.
- Ensuring staff are regularly trained to an appropriate level and comply with this policy.

The Deputy Head deputises for the Headteacher.

School Business Manager

The School Business Manager, Mrs Louise Smith, has the following responsibilities: -

- Promoting compliance and assisting the school and its staff with this policy and all relevant Data Protection legislation;
- Liaising with the Data Protection Officer when auditing data protection policies and procedures;
- Carrying out Data Protection Impact Assessments for any new process;
- Producing and publishing the Publication Scheme;
- Processing requests for information and responding to the requester;
- Maintaining the Inventory of Records and Retention Schedule, and associated records;
- Carrying out request for information for Internal Reviews (complaint investigations).

Contact details: bm.crosbyprimary@northlincs.gov.uk

Data Protection by Design and Default

We put measures in place to show that we have integrated data protection into all of our data processing activities, including:

- Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge.
- Only processing personal information that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law.
- Completing a Data Protection Impact Assessment (DPIA) where the school's processing of personal information presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on this process).
- Integrating data protection into internal documents, any related policies and privacy notices.
- Regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters; we will also keep a record of attendance.
- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant.
- Maintaining records of our processing activities, including:

- For the benefit of data subjects, making available the name and contact details of our school and DPO and all information we are required to share about how we use and process their personal information (via our privacy notices).
- For all personal information that we hold, maintaining an internal record of the type of data, data subject, how and why we are using the data, any third-party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure.

Data Protection Impact Assessments

An annual risk assessment will be carried out by the school on all major information assets, such as IT systems, record storage facilities and processes to assess and record the risk to personal information. These will be documented along with any action required to reduce the risk to personal information. The same risk assessment will be carried out before the introduction of new systems and ways of working. These risk assessments are called Data Protection Impact Assessments (DPIA).

- A Data Protection Impact Assessment (DPIA) is a process to help identify and minimise the data protection risks of a project. We use the ICO screening checklists to help decide when to do a DPIA.
- A DPIA is carried out for processing that is likely to result in a high risk to individuals. This includes some specified types of processing.
- A DPIA is carried out for any other major project which requires the processing of personal information.
- A DPIA will:
  - describe the nature, scope, context and purposes of the processing;
  - assess necessity, proportionality and compliance measures;
  - identify and assess risks to individuals; and
  - identify any additional measures to mitigate those risks.
- To assess the level of risk, we consider both the likelihood and the severity of any impact on individuals. High risk could result from either a high probability of some harm, or a lower possibility of serious harm.
- We consult the Data Protection Officer and, where appropriate, individuals and relevant experts.
- We may seek assistance from any processors of the data.
- If a high risk is identified and cannot be mitigated, we consult the ICO before starting the processing.

Records Management

Data Security and Storage of Records

In order to protect personal information and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage:

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal information are kept under lock and key when not in use.
- Papers containing confidential personal information must not be left on office and classroom desks, on staffroom tables, pinned to notice/display boards, or left anywhere else where there is general access.
- Passwords of 'three random words' in line with recommendations by the National Cyber Security Centre https://www.ncsc.gov.uk/ are recommended to access school computers, laptops and other electronic devices. Staff and pupils are reminded to change their passwords at regular intervals.
- Encryption software is used on removable media, such as USB devices.
- Staff, pupils or governors who store personal information on their own devices are expected to follow the same security procedures as for school-owned equipment (see Acceptable Use of ICT Policy).

- Where we need to share personal information with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected.

Inventory of Records and Retention Schedule
An Inventory of Records and Retention Schedule is provided to keep a log of what records are held. The Inventory of Records and Retention Schedule is updated on a regular basis.

What is a Record?
It is important, to make a distinction between what is and is not a record. According to the ISO 15489 standard for the management of records, a record is:

> *"Information created, received, and maintained as evidence and information by an organisation or person, in pursuance of legal obligations or in the transaction of business."*

Essentially, it is a record of the school's business that requires effective management and preservation. Examples of records include:

- Correspondence.
- Meeting minutes.
- Education Record

A **non-record**, is an item of information that does not require the same rigour of management as that required for records and is of immediate value only. Non-records can be disposed of once they have served their useful purpose.

Management of electronic and/or email records
The principles that apply to the management of electronic records are generally the same as those for the management of paper records. Effective electronic record keeping requires:

- The rules around the retention and disposal of records in IT systems and email systems are the same as those for other records in that these records, in that these records should be disposed of when they should no longer be kept.
- Audit trails may be used to show who has accessed, moved or deleted records in IT systems.
- Emails can sometimes be records and can be disclosable in response to requests for information.

Sometimes other people will have been copied into emails and therefore care is needed to ensure all copies are disposed of when the record should no longer be kept.

Sometimes emails should be removed from the email system and stored in another electronic or paper filing system.

If the email has an attachment and the text of the email adds to the record, care needs to be taken to ensure both parts of the record are kept together.

Records Management Lifecycle
All information goes through a lifecycle, from its creation to its disposal.

- Pre creation – deciding what information needs to be captured as a record and how.
- Create/receive – information that needs to be kept as a record can enter the school in many ways. Some is created within; some comes from external sources.
- Index/classify – the addition of descriptive information to records.
- Process – records may need to be processed at any point (have something done to them).
- Store/manage – how and where they should be stored.
- Retrieval - the finding of stored records by those who are entitled to search for them.
- Destroy or Preserve – if records do not need to be retained permanently, and have reached the disposal date they should be destroyed.

Record maintenance and storage

The record keeping system will provide suitable storage with the necessary protection and it will be kept up to date in accordance with the Inventory of Records and Retention Schedule. Records that contain sensitive or personal information should be allocated immediately to the correct location.

Information Handling

Storage

- Information must not be put at risk of damage or theft, and must be stored securely and access allowed only to those who need, it for legitimate purposes and in accordance with the Data Protection Act 2018. For example:
    - Records should be stored in secure buildings with access controls to the building, specific floors and individual offices.
    - The location of any stored records should be sited to avoid unauthorised access, damage, theft and interference.
    - Stored records must not be removed or moved to another location without authorisation from the Headteacher or deputy.
    - Electronic information must to be stored on the school network unless alternative storage (e.g. Cloud) is authorised.

Communication

- Extra care should be taken when printing sensitive information. Print release security controls will be used whenever possible but in any areas without multi-functional devices ensure printed sensitive information is not left unattended.
- Voicemail may contain personal and sensitive information and therefore passwords should be kept secure.
- File Sharing products or 'apps' that are not approved by IT Services must not be used for school business.

Portable hardware including laptops, mobile devices & tablets

- Equipment taken off site must be locked away and kept out of sight when left unattended.
- Users shall ensure that unauthorised persons are not able to view school's information on portable devices and shall protect access by locking computers when unattended.

Records Management

- Records are a key resource for the effective operation and accountability of the school. It is also recognised that some records will over time become of historical value and need to be identified and preserved accordingly.
- Hardcopy records that do not need day to day access should be stored away from the immediate workplace.
- Any hard copy or electronic records temporarily stored away from the usual storage location must be returned there as soon as is practicable.

Removable media

- To prevent data loss, the use of any removal media must be approved by the Headteacher or deputy with a strong business case for use.
- Staff must only use mobile media to store or transfer personal and sensitive school information if there is no other more secure means available e.g. Government secure GCSx email.
- Only media with a sufficient level of encryption may be used to temporarily hold personal and sensitive school information.

Office/desk security

- Staff should maintain a clear desk policy and ensure that all personal and sensitive information is kept secure:
    - To minimise the risk of mixing up information and accidentally releasing it to someone who should not see it only information relating to the current task should be on the working area of the desk at any one time.
    - Personal and sensitive information including phone numbers, passwords, financial records, notes on meeting times, places and subjects must not be left unattended
    - Mobile phones can contain sensitive personal information and have their call histories compromised and therefore should be kept secure using a pin number and/or passcode at all times and not left unattended
    - Keys and access cards should not be left unattended as they can give intruders access to restricted areas
    - Positioning of desks, furniture and visual display boards should be carefully considered to prevent

Information Handling

sensitive information being visible to unauthorised people.
- Personal and sensitive information should not be left on white boards or notice boards.
- When leaving desks for short periods all users must use 'Ctrl, Alt and Delete' to lock computers. When leaving desks for long periods users must ensure they are logged off the network.

Retention and disposal

The Inventory of Records and Retention Schedule sets out the minimum time records should be kept for and the action that should be taken at the end of the retention period. This is based on Local Government Association and Information and Records Management Society (IRMS) guidelines.

Reaching the end of the minimum retention period does not always mean the record should be destroyed. In some cases, the record may be retained longer or transferred to permanent archive. Records being retained longer by the school are assigned a further review date and this should be updated at each future review.

All records will be disposed of in accordance with the Inventory of Records and Retention Schedule. Any records being considered for disposal outside of the schedule disposal date must be discussed with the Headteacher prior to destruction.

The aim of the retention and disposal process is to ensure that:

- Personal information that has become inaccurate or out of date, where we cannot or do not need to rectify or update it, or is no longer needed will be disposed of securely.
- The review date at the end of the retention period is captured when creating records or receiving records.
- Records reaching the end of the minimum retention period are reviewed and a decision made about whether to dispose of the record or keep it longer.
- The Inventory of Records and Retention Schedule is kept updated to reflect disposal, archiving or further retention decisions taken.
- Records subject to an outstanding request for information or legal proceedings will not be destroyed until after the request has been answered and/or the legal proceedings are completed.
- Destruction will be carried out in accordance with its level of sensitivity and in line with the retention and disposal of records procedures.
- We will shred paper-based records, and overwrite or delete electronic files. We use a third party to safely dispose of records and hard drives on the school's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law. Waste transfer notes and certificates of destruction are retained in these instances.

Security Incidents and Data Breaches

School staff must ***immediately*** inform the Headteacher or School Business Manager if they suspect there has been or might be a security incident that could result in the school's personal information being lost or seen by someone who should not see it. The school will make all reasonable endeavours to ensure that there are no personal data breaches.

The following are factors that may lead to a security incident:

- Negligence or human error;
- Unauthorised or inappropriate access, such as accessing information you are not permitted to see or using someone else's password;
- Loss or theft of information or equipment;

- Systems or equipment failure;
- Environmental factors, such as fire or flooding;
- Accessing information without a business reason to do so;
- Insufficient physical security;
- Insufficient access controls;
- Lack of training;
- Hacking;
- 'Blagging' or 'social engineering' in order to gain access to information.

The school will immediately investigate in order to keep damage to a minimum and to reduce the likelihood of a recurrence.

Data Breaches

A data breach can be broadly defined as a security incident, either accidental or deliberate, that has affected the confidentiality, integrity or availability of personal data.

A personal data breach is whenever any personal data is:

- lost, destroyed, altered, corrupted or disclosed;
- accessed or passed on without proper authorisation;
- made unavailable and this unavailability has a significant negative effect on individuals.

In the unlikely event of a suspected data breach, we will follow the procedure set out in below.

When appropriate, we will seek advice about the suspected data breach from the ICO. Any confirmed data breach must be reported to the ICO within 72 hours.

Data Breach Procedure

This procedure is based on guidance on personal data breaches produced by the ICO.

- On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the DPO
- The DPO will investigate the report, and determine whether a breach has occurred. To decide, the DPO will consider whether personal information has been accidentally or unlawfully:
    - Lost
    - Stolen
    - Destroyed
    - Altered
    - Disclosed or made available where it should not have been
    - Made available to unauthorised people
- The DPO will alert the Headteacher and the chair of governors
- The DPO will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary.
- The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen
- The DPO will work out whether the breach must be reported to the ICO. This must be judged on a case-by-case basis.

Data Breach Procedure

- To decide, the DPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:
    - Loss of control over their data
    - Discrimination
    - Identify theft or fraud
    - Financial loss
    - Unauthorised reversal of pseudonymisation (for example, key-coding)
    - Damage to reputation
    - Loss of confidentiality
    - Any other significant economic or social disadvantage to the individual(s) concerned

  If it's likely that there will be a risk to people's rights and freedoms, the DPO must notify the ICO.
- The DPO will document the decision (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored by the School DPO
- Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website within 72 hours. As required, the DPO will set out:
    - A description of the nature of the personal information breach including, where possible:
        - The categories and approximate number of individuals concerned
        - The categories and approximate number of personal information records concerned
    - The name and contact details of the DPO
    - A description of the likely consequences of the personal information breach
    - A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned
- If all the above details are not yet known, the DPO will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible
- The DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPO will promptly inform, in writing, all individuals whose personal information has been breached. This notification will set out:
    - The name and contact details of the DPO
    - A description of the likely consequences of the personal information breach
    - A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned
- The DPO will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies
- The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:
    - Facts and cause
    - Effects
    - Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)
- Records of all breaches will be stored by the School DPO
- The DPO and Headteacher will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible

Training
All staff are provided with data protection training as part of their induction process. Staff are updated, at least annually, regarding their responsibilities under data protection law. Data protection will also form part of continuing professional development, where changes to legislation, guidance or the school's processes make it necessary.

Complaints
If anyone considers their information request has not been dealt with in a satisfactory manner it will be reviewed using the School Complaints Procedure.

How to appeal against the outcome of an Information Complaint
Where the school has Internally Reviewed a complaint about the FOIA, EIR, DPA or RPSI and you are not satisfied, you may appeal to the Information Commissioner's Office, as follows:

Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF; Telephone: 0303 123 1113 or 01652 545700 - www.ico.gov.uk

Appeals about the Education Record in relation to a maintained school should be directed to the Department of Education – Schools Complaints Unit (Complain about a School or Childminder) - https://www.gov.uk/complain-about-school/state-schools

Links with other policies and procedures
This policy is supported by other policies, standards and procedures, including:

- Privacy Notices
- Safeguarding and Child Protection Policy
- Online Safeguarding Policy
- Acceptable Use of Information and Communication Technology
- Complaints Procedure
- Publication Scheme
- Information and Records Management Society (IRMS) Records Management Toolkit for Schools
- Department for Education - Schools Complaints Unit - Complain about a School or Child-minder https://www.gov.uk/complain-about-school/state-schools
- Department for Education – Education Funding Agency https://www.gov.uk/government/organisations/education-funding-agency

Monitoring arrangements
The Governing Body is responsible for monitoring and reviewing this policy.

The Data Protection Officer (DPO) is responsible for overseeing the implementation of this policy. Working with the school as the data controller the DPO is also responsible for monitoring compliance with data protection law, developing related policies and guidelines, where applicable.

This policy will be reviewed every 3 years. Last review Summer 2021. Next review Summer 2024.

Appendix 1: Legislation

Legislation for Standards and Compliance

Data Protection Act 2018
Principles setting out how we must deal with personal information and the right for individuals to gain access to the personal information that is held about them.

Freedom of Information Act 2000
Public access rights to all information held, other than that which is exempt. In addition, the Section 46 Code of Practice gives guidance on good practice in records management.

Environmental Information Regulations 2002
Public access rights to environmental information.

Local Government Act 1972
Section 224 of the Act requires local authorities to make proper arrangements in respect of the records they create.

Public Records Acts of 1958 and 1967
All public bodies have a statutory obligation to keep records in accordance with the Public Records Act. This places the responsibility on government departments and other organisations within the scope of the Act for making arrangements for selecting those of their records, which ought to be permanently preserved, and for keeping them in proper conditions. Parts of this Act have been superseded – particularly by the FOIA.

Limitation Act 1980
Has particular relevance to applying appropriate retention periods. For example, in regard to financial records, the Act "provides that an action to recover any sum recoverable by any enactment shall not be brought after the expiration of six years from the date on which the cause of the action accrued".

Health and Safety at Work Act 1974
Influences how long records relating to Health and Safety incidents should be retained.

Human Rights Act 1998
Particular relevance in relation to an individual's right to privacy.

Information Security Management System Requirements: ISO 27001
This is complementary to ISO 17799 and defines the requirements for an Information Security Management System (ISMS). This, effectively, describes the process for creating an ISMS, implementing and managing the governance and controls described in ISO 17799.

Code of Practice for Legal Admissibility: BIP 0008
Provides a framework and code of good practice for the implementation and operation of information storage systems, whether or not any information held therein is ever required as evidence in event of a dispute.

Retention Guidelines for Schools - Records Management Society
Guidance for schools on the retention and disposal of records.

Education Act 2011
Sets out educational policy.

Education (Pupil Information) Regulations 2008 (PIR)
Sets out how a pupil's Education Record must be maintained and who it can be disclosed to.

Appendix 2: Exemptions and Exceptions

Data Protection Exemptions

The DPA exemptions are complex. In some cases, the exemption removes an individual's right to make a Subject Access Request (SAR), in other cases the exemption means personal information can be released to a third party, other exemptions mean there is no requirement to provide a privacy notice and a further set of exemptions mean that there is no need to register with the Information Commissioner.

The DPA exemptions that are most applicable to schools are summarised below:

1) Section 29 - Crime and Taxation
   If information is processed for the purposes of the prevention or detection of crime; the apprehension or prosecution of offenders; the assessment or collection of tax or duty it is exempt from principal one of the DPA and also from the Data Subject's right of access.
   This also means that if information is required for such purposes, then it may be disclosed to a third party.
2) Section 34 – Disclosures Required by Law
   If an organisation is required to disclose personal information under any UK enactment, any rule of common law or by an order of a court or tribunal it is exempt from principle one of the DPA. This means for these purposes it could be disclosed to a third party.
3) Section 35 – Legal Advice and Proceedings
   If an organisation is required to disclose personal information in connection with ongoing or prospective legal proceedings, to allow the obtaining of legal advice or to establish, exercise or defend legal rights it is exempt from principle one of the DPA. This means for these purposes it could be disclosed to a third party.
4) Schedule 7 – Confidential References
   Personal information in a confidential reference given by an organisation is exempt from a Data Subject's right of access. This does not apply to references received by an organisation.
5) Schedule 7 – Management Information
   Personal information that is being used for management forecasting or planning is exempt from a Data Subject's right of access if release is likely to harm the organisation.
6) Schedule 7 – Negotiations
   Personal information that is part of a record of the organisations intentions in negotiations is exempt for a Data Subject's right of access if release is likely to harm the negotiations.
7) Section 30– Personal Information in Educational Records
   Personal information that is part of an Educational record is exempt for a Data Subject's right of access if release is likely to cause serious harm to the physical or mental health of the data subject or someone else.
8) Schedule 7 – Examination Marks and Scripts
   Personal information in the form of exam marks is exempt from a Data Subject's right of access until 40 days after publication of results or 5 months after the request has been made, whichever is sooner.
   Personal information in the form of a pupil's responses to exam questions is exempt from a Data Subject's right of access. Comments made by an examiner are not exempt.

Pupil Information Regulation Exemptions

The following exemptions exist under the Pupil Information Regulations and they allow information to be withheld in certain situations when requests are made for information in an Education Record held by a maintained school.
Below is a summary of these exemptions:

1) Data Protection Act 2018
   Information can be withheld where the school is able to withhold it under the Data Protection Act 2018.
2) Serious Harm to Physical or Mental Health
   Information can be withheld if releasing it would be likely to cause serious physical or mental harm to the requester or another person.
3) Child Abuse
   Information can be withheld about whether the child is or has been subject to or may be at risk of child abuse, where disclosure would not be in the best interests of the child.

4) Court Information
Information provided to a court can be withheld.

Freedom of Information Exemptions

The Act has a series of exemptions that may allow information to be withheld, as follows:
'Absolute' exemptions – information will not be disclosed under any circumstances.

'Qualified' exemptions - a public interest test will be carried out and the information will only be withheld if the public interest in not disclosing is greater than the public interest in disclosing.
Some of the 'qualified' exemptions are also subject to a prejudice test, which must be carried out before the information can be considered exempt. This test considers whether harm will or is likely to be caused if the information is released.

Absolute Exemptions

1. Information accessible to the applicant by other means (section 21)
2. Security Matters (Section 23)
3. Court Records (Section 32)
4. Parliamentary Privilege (Section 34)
5. Conduct of public affairs in relation to parliament (Section 36)
6. Communications with Her Majesty and awarding of honours (Section 37)
7. Personal information (Section 40)
8. Information provided in confidence (Section 41)
9. Other legal prohibitions on disclosure (Section 44)

Qualified Exemptions

1. Information intended for future publication (Section 22)
2. National security (Section 24) – prejudice based
3. Defence (Section 26) – prejudice based
4. International relations (Section 27(1)) – prejudice based
5. International relations – relating to information obtained from another state (Section 27(2))
6. Relations with the UK (Section 28) – prejudice based
7. The economy (Section 29) – prejudice based
8. Investigations and proceedings conducted by public authorities (Section 30)
9. Law enforcement (Section 31) – prejudice based
10. Audit functions (Section 33) – prejudice based
11. Formulation of government policy (Section 35)
12. The effective conduct of public affairs (Section 36) – prejudice based
13. Communications with Her Majesty – to the extent not absolute (Section 37)
14. Health and safety (Section 38) – prejudice based
15. Environmental information (Section 39)
16. Personal information – to the extent not absolute (Section 40)
17. Legal professional privilege (Section 42)
18. Commercials interests – which apply to trade secrets (Section 43(1))
19. Commercial interests (Section 43(2)) – prejudice based.

Environmental Information Regulation Exceptions

The Regulations have a series of exceptions that may allow information to be withheld, as follows:

'Absolute' exemptions – there is one exception that falls into this category that applies to requests for personal information and it means that this information will not be disclosed under any circumstances.

'Qualified' exemptions - a public interest test will be carried out and the information will only be withheld if the public interest in not disclosing is greater than the public interest in disclosing.

Information on emissions into the environment is subject to more limited exceptions than other environmental information.

Under the Regulations there is an express presumption in favour of disclosure meaning that information should be made available unless there is a very strong reason for it not to be.

Regulation 12(3)

1) Personal information.
   Applies where the personal information of a third party is requested.

Regulation 12(4) – Information can be withheld if:

2) Information is not held when the request is received.
   Applies if the information is not held at the point the request is made.
3) Request is manifestly unreasonable.
   The request is considered vexatious or is so large as to be unreasonable.
4) Request is too general.
   Can only be used after advice and assistance has been offered to the requester to help refine or clarify the request.
5) Information which is unfinished or in the course of being completed.
   Where information is intended for future publication where the expected date of completion can be advised.
6) Request involves the disclosure of internal communications.
   To protect information created during internal thinking time.

Regulation 12(5) – Information can be withheld if:

7) Disclosure would affect international relations, defence, national security or public safety.

Applies were harm could be caused by releasing the specified information.

8) Disclosure would affect the course of justice, the ability of a person to receive a fair trial or ability of a public authority to conduct or criminal or disciplinary enquiry. Where releasing information would harm the course of justice or the right of an individual to a fair trial.
9) Intellectual property rights.
   If the release of information could seriously damage the rights given under trademarks and patents, for example
10) The confidentiality of the proceedings of a public authority where such confidentiality is protected by law.
    To be used where confidentiality is protected by law and not where information is simply marked ‘confidential’.
11) Commercial or industrial confidentiality where such confidentiality is provided by law to protect a legitimate economic interest. Where such confidentiality is provided by law to protect a legitimate economic interest and it can be proven that the person or organisation would suffer a real commercial or competitive disadvantage if the information were released.
12) The interests of the supplier of the information.
    Where the provider of the information did so voluntarily and was not under (and could not have been put under) a legal obligation to supply the information and also did not give consent to its disclosure.
13) The protection of the environment to which the information relates.
    Releasing the information could have a detrimental effect on the environment.

It is also our right to refuse requests from the Data Subject, when those requests have been repeated or similar and unreasonably close in time. Also if there would be a "disproportionate effort" involved in our responding.

Appendix 3: Information Request Charging

Information Request Charging

1) Freedom of Act 2000 and Environmental Information Regulation Charges

a) Freedom of Information Fee Limit Calculation (Not applicable to EIR):

This fee limit is reached under FOIA if it is estimated that the time taken to carry out the following four activities would exceed 18 hours of employee time, based on a £25 per hour rate regardless of job grade.

The same calculation is used to determine the fee if a request remains over the fee limit but it is agreed that we proceed with the request on payment of a fee by the applicant: -

- Determining whether the information requested is held;
- Locating the information;
- Retrieving the information;
- Extracting the information to be disclosed (including the cost of materials used for editing redacting information, but not including staff time for this task).

The following costs cannot be included in this calculation: -

- Checking whether the request meets the requirements of the FOIA;
- Locating information due to poor records management practice;
- Considering the application of an exemption;
- Applying a public interest test;
- Obtaining internal or external legal advice;
- Considering whether a request is vexatious or repeated;
- Repeating an activity already undertaken;
- Employee time for editing or redacting information;
- Obtaining authorisation to provide information;
- Calculating any fees to be charged;
- Issuing a fees notice;
- Providing advice and assistance.

b) Charges under other Legislation

If information is requested where other legislation permits a charge will be chargeable.

c) Publication Scheme

Information made available through the school's Publication Scheme where a charge is published will be chargeable.

d) Disbursement Costs

A reasonable charge may be made to cover the actual cost of communicating information to the requester. These charges can be made up of the cost of the following (other similar charges may also be included but it should be noted that a school is not permitted to charge for staff time):

- Reproducing any document containing the information, eg printing or photocopying;
- Postage and other forms of transmitting the information;
- Providing information in a particular format where the applicant has expressed a preference for the means of communication and where this is reasonably practicable.

If these charges are applied the school will publish details of how these charges are calculated, times when they will not be applied, what will not be included in the calculation and when refunds would be considered.

e) Data Protection Section 29 and Section 35 Requests

An administration fee may be charged for these requests and will be published by the school.

2) Requests to Re-Use Information

Any charges associated with requests to re-use information already made accessible, will be advised on application.

Information Request Charging

Where possible in the spirit of transparency information will be made available for re-use free of charge.

3) Data Protection Act 2018 Charges
A charge of £10 will be made for each Subject Access Request for personal information that is not part of the Education Record.

If any part of the request relates to the Education Record that is held at a maintained school, please see the Pupil Information Regulation Charges section.

4) Pupil Information Regulation 2008 Charges
If any part of the request relates to the Education Record held by a maintained school, the charge will depend on the number of pages being released on a sliding scale of £1 for 1-19 pages to £50 for 500+ pages.

There is no charge to inspect an Education Record at a maintained school, if no copies are required.

Appendix 4: Information Sharing Statement

Information Sharing Statement for inclusion in record transfers

Crosby Primary recognises that effective information sharing between parents, schools, colleges and local authorities is critical to ensuring that all children are safe and receiving suitable education. We understand that effective sharing of information between professionals and local agencies is essential for effective identification, assessment and service provision. Information sharing is vital to safeguarding and promoting the welfare of children.

In order to fulfil our statutory duties, we follow guidance provided in the documents:

- 'Keeping Children Safe in Education: Statutory guidance for schools and Colleges - January 2021';
- 'Information Sharing: Advice for practitioners providing safeguarding services to children, young people, parents and carers - July 2018';
- 'Working Together to safeguard children: A guide to inter-agency working to safeguard and promote the welfare of children - July 2018'.

We expect that all who share information will follow guidance in the documents above. We also expect that assurances be given that any personal information provided will be processed in a manner that ensures appropriate security in accordance with The UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA 2018).