Fred Nicholson School

GDPR & Data Retention Policy

'Building for Successful Futures'

Formally adopted by the Governing Board of	Fred Nicholson School
Chair of Governors	Hilary Bradshaw
Policy Holder	Headteacher
Policy Contributor	SBM - Sue Martin
Last updated	Autumn 2024
To be Reviewed	Autumn 2025

Statutory Policy	**Y**	**Published on Website**	**Y**

This policy is based on a model policy from The Key for School Leaders, developed with the NAHT and approved by Forbes Solicitors.

Any updates and amendments to government legislation or guidance from the Education HR Service automatically supersede this school policy prior to ratification by the Governing Body.

This policy applies to all areas of school.

Contents

Appendices

GDPR & Data Retention Policy

We want our pupils to:

Be eager, excited, curious and engaged in learning.
Have a sense of self and are happy, confident and emotionally healthy.
Be able to co-operate and communicate socially.
Be healthy and safe.
Feel equipped to make life choices, recognize their own achievement, take responsibility for themselves and behave in a way that enhances their wellbeing and the wellbeing of others.

1. Scope of Policy

This policy reflects our school's commitment to the General Data Protection Regulation (UK GDPR) the EU GDPR was incorporated into UK legislation, with some amendments, by **The Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2020**

It is based on guidance published by the Information Commissioner's Office (ICO) on the **UK GDPR.**

It meets the requirements of the **Protection of Freedoms Act 2012** when referring to our use of biometric data.

It also reflects the ICO's **guidance** for the use of surveillance cameras and personal information.

In addition, this policy complies with regulation 5 of the **Education (Pupil Information) (England) Regulations 2005**, which gives parents the right of access to their child's educational record.

2. Definitions

As defined by the UK GDPR:

- **personal data** means any information relating to an identified or identifiable natural person in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or by one or more factors specific to the

- physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;
- **Data controller** means 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. Our school processes personal data of parents, pupils, staff, governors, visitors and others, and therefore, is a data controller.
  The school is registered with the ICO and has paid its data protection fee to the ICO, as legally required.
- **data subject** means the identified or identifiable individual whose personal data is held or processed.
- **Data processing** means any operation or set of operations which is performed on personal data or on sets of personal data, automated or manual, such as collection, recording, School, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;
- **Data processor** means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;
- **Data recipient** means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance UK GDPR law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing;

- **third party** means 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;
- **consent** of the data subject 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 relating to him or her;
- **personal data breach** means 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;
- **special categories** of personal data means personal data:
  - revealing racial or ethnic origin,
  - revealing political opinions,
  - revealing religious or philosophical beliefs or trade union membership,

- the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person,
- data concerning health (physical or mental) or data concerning a natural person's sex life or sexual orientation shall be prohibited;

- **data breach**: an incident or event in which personal and/or confidential data:
  - has potentially been viewed or used by an individual unauthorised to do so;
  - has had its integrity compromised;
  - is lost or is unavailable for a significant period.

Further definitions can be found in **Appendix A**

3. Roles and responsibilities

This policy applies to **all staff** employed by our school, and to external Schools or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action.

3.1 Governing board

The governing board has overall responsibility for ensuring that our school complies with all relevant data protection obligations.

3.2 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. The School shall support the DPO in performing their responsibilities by providing resources necessary to carry out those tasks and access to personal data and processing operations.

The School shall ensure that the DPO does not receive any instructions regarding the exercise of their tasks. They shall not be dismissed or penalised by the controller or the processor for performing his tasks.

Full details of the DPO's responsibilities are set out in the DPO job description. The Data Protection Officer shall maintain his or her expert knowledge. They will provide an annual report of their activities directly to the governing board and, where relevant, report to the board their advice and recommendations on school data protection issues. The DPO shall be bound by secrecy or confidentiality concerning the performance of his or her tasks.

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

Our DPO is the School Business Manager, currently Sue Martin and is contactable via smartin@frednicholson.school

3.3 Headteacher

The headteacher acts as the representative of the data controller on a day-to-day basis.

3.4 All staff

Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Informing the school of any changes to their personal data, 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 data or keeping personal data secure
    - If they have any concerns that this policy is not being followed
    - If they are unsure whether or not they have a lawful basis to use personal data 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 data outside the UK
    - 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 data with third parties

4. Data Principles & Collecting personal data

The UK GDPR is based on data protection principles that our school must comply with. The school is committed to the principles relating to processing of personal data, in that personal data will be:

- **processed lawfully, fairly and in a transparent manner** in relation to the data subject;
- **collected for specified, explicit and legitimate purposes** and not further processed in a manner that is incompatible with those 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;**
- **kept in a form which permits identification of data subjects for no longer than is necessary**;

- **processed in a manner that ensures appropriate security of the personal data**.

This policy sets out how the school aims to comply with these principles.

4.1 Lawful processing, fairness & transparency

We will only process personal data where we have one of 6 'lawful bases' (legal reasons) to do so under data protection law:

- the data subject (or their parent/carer when appropriate in the case of a pupil) has given **consent** to the processing of his or her personal data for one or more specific purposes;
- processing is necessary for the **performance of a contract** to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
- processing is necessary for compliance with a **legal obligation** to which the controller is subject;
- processing is necessary in order to protect the **vital interests** of the data subject or of another natural person i.e. to save someone's life;
- 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 data controller.

For special categories of personal data, we will also meet one of the special category conditions for processing under data protection law:

- The individual (or their parent/carer when appropriate in the case of a pupil) has given **explicit consent**
- The data needs to be processed to perform or exercise obligations or rights in relation to **employment, social security or social protection law**
- The data needs to be processed to ensure the **vital interests** of the individual or another person, where the individual is physically or legally incapable of giving consent
- The data has already been made **manifestly public** by the individual
- The data needs to be processed for the establishment, exercise or defence of **legal claims**
- The data needs to be processed for reasons of **substantial public interest** as defined in legislation
- The data needs to be processed for **health or social care purposes**, and the processing is done by, or under the direction of, a health or social work professional or by any other person obliged to confidentiality under law

- The data needs to be processed for **public health reasons**, and the processing is done by, or under the direction of, a health professional or by any other person obliged to confidentiality under law
- The data needs to be processed for **archiving purposes**, scientific or historical research purposes, or statistical purposes, and the processing is in the public interest

For criminal offence data, we will meet both a lawful basis and a condition set out under data protection law. Conditions include:

- The individual (or their parent/carer when appropriate in the case of a pupil) has given **consent**
- The data needs to be processed to ensure the **vital interests** of the individual or another person, where the individual is physically or legally incapable of giving consent
- The data has already been made **manifestly public** by the individual
- The data needs to be processed for or in connection with legal proceedings, to obtain legal advice, or for the establishment, exercise or defence of **legal rights**
- The data needs to be processed for reasons of **substantial public interest** as defined in legislation

Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law.

We will always consider the fairness of our data processing. We will ensure we do not handle personal data in ways that individuals would not reasonably expect, or use personal data in ways which have unjustified adverse effects on them.

4.2 Limitation, minimisation and accuracy

We will only collect personal data for specified, explicit and legitimate reasons. We will explain these reasons to the individuals when we first collect their data.

If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so, and seek consent where necessary.

Staff must only process personal data where it is necessary in order to do their jobs.

We will keep data accurate and, where necessary, up to date. Inaccurate data will be rectified or erased when appropriate.

In addition, when staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with the school's record retention schedule.

5. Data Sharing

Data will be shared with third parties only where a lawful basis exists. We will not normally share personal data with anyone else without consent, but there are certain circumstances where we may be required to do so. These include, but are not limited to, situations where:

- There is an issue with a pupil or parent/carer that puts the safety of our staff at risk
- We need to liaise with other agencies – we will seek consent as 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 UK data protection law
- Establish a contract with the supplier or contractor to ensure the fair and lawful processing of any personal data we share
- Only share data that the supplier or contractor needs to carry out their service

We will also share personal data with law enforcement and government bodies where we are legally required to do so.

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

Data may be shared for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes. In this case, efforts will be made to ensure the minimum data required is shared and if possible, anonymised prior to sharing.

Where data is shared with third-party processors, they will only process data with the explicit instructions (either contractual or through a data sharing agreement) of the School and shall not hold or process the data for any other purpose. The minimum data required for the processing task will be provided for the processing.

Where we transfer personal data internationally, we will do so in accordance with UK data protection law.

6. Information Commissioner's Office

For the purposes of data protection, The School is a data controller; responsible for the determination of the purposes and means of the processing of personal data and where the purposes and means of such processing takes place. As such, The School is supervised by the Information Commissioner's Officer and will pay the data protection fee required by law.

The Data Protection Officer will be the principal point of contact with the Information Commissioner's Office.

7. Subject access requests and other rights of individuals

7.1 Subject access requests

The School is committed to:

- Ensuring that individuals' rights to their own personal information can be appropriately exercised;
- Providing adequate training for staff to recognise and handle subject access requests;
- Ensuring that everyone handling personal information knows where to find further guidance on individuals' rights in relation to their own personal information;
- Ensuring that queries about individuals' rights to their own personal information are dealt with effectively and promptly;
- Being fair and transparent in dealing with a subject access request;
- Logging all subject access requests to assist the Information Commissioner's Office with any complaints related to subject access as well as identifying any issues that may assist in the identification of new data handling processes and training requirements.

All staff are responsible for ensuring that any request for information they receive is dealt with in line with the requirements of the GDPR and in compliance with this policy.

All staff have a responsibility to recognise a request for information and ensure it is passed to the responsible member of staff and/or the Data Protection Officer within two working days.

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

- Confirmation that their personal data is being processed
- Access to a copy of the data
- The purposes of the data processing

- The categories of personal data concerned
- Who the data has been, or will be, shared with
- How long the data will be stored for, or if this isn't possible, the criteria used to determine this period
- Where relevant, the existence of the right to request rectification, erasure or restriction, or to object to such processing
- The right to lodge a complaint with the ICO or another supervisory authority
- The source of the data, if not the individual
- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual
- The safeguards provided if the data is being transferred internationally

Subject access requests can be submitted in any form, but we may be able to respond to requests more quickly if they are made in writing and include:

- Name of individual
- Correspondence address
- Contact number and email address
- Details of the information requested

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

7.2 Children and subject access requests

Personal data about a child belongs to that child, and not the child's parents or carers. For a parent or carer to make a subject access request with respect to their child, the child must either be unable to understand their rights and the implications of a subject access request, or have given their consent.

Primary school age children:

Children below the age of 12 are generally not regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of pupils at our school may be granted without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

Secondary schools age children:

Children aged 12 and above are generally regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of pupils at our school may not be granted without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

7.3 Responding to subject access requests

When responding to requests, we:

- May ask the individual to provide 2 forms of identification
- May contact the individual via phone to confirm the request was made
- Will respond without delay and within 1 month of receipt of the request (or receipt of the additional information needed to confirm identity, where relevant)
- Will provide the information free of charge
- May tell the individual we will comply within 3 months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within 1 month, and explain why the extension is necessary

We may not disclose information for a variety of reasons, such as if it:

- Might cause serious harm to the physical or mental health of the pupil or another individual
- Would reveal that the child is being or has been abused, or is at risk of abuse, where the disclosure of that information would not be in the child's best interests
- Would include another person's personal data that we can't reasonably anonymise, and we don't have the other person's consent and it would be unreasonable to proceed without it
- Is part of certain sensitive documents, such as those related to crime, immigration, legal proceedings or legal professional privilege, management forecasts, negotiations, confidential references, or exam scripts

If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee to cover administrative costs. We will take into account whether the request is repetitive in nature when making this decision.

When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO or they can seek to enforce their subject access right through the courts.

7.4 Other data protection rights of the individual

In addition to the right to make a subject access request (see above), and to receive information when we are collecting their data about how we use and process it, individuals also have the right to:

- Withdraw their consent to processing at any time
- Ask us to rectify, erase or restrict processing of their personal data (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Object to processing which has been justified on the basis of public interest, official authority or legitimate interests
- Challenge decisions based solely on automated decision making or profiling (i.e. making decisions or evaluating certain things about an individual based on their personal data with no human involvement)
- Be notified of a data breach (in certain circumstances)
- Make a complaint to the ICO
- Ask for their personal data 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.

7.5 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.

If the request is for a copy of the educational record, the school may charge a fee to cover the cost of supplying it.

This right applies as long as the pupil concerned is aged under 18.

There are certain circumstances in which this right can be denied, such as if releasing the information might cause serious harm to the physical or mental health of the pupil or another individual, or if it would mean releasing exam marks before they are officially announced.

8. CCTV

We use CCTV in various locations around the school site to ensure it remains safe. We will follow the ICO's guidance for the use of CCTV, and comply with data protection principles.

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 Premises Manager.

9. 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 including social media. We will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil.

Parents and carers are requested not to take any photographs and videos at school events for their own personal use unless in an agreed situation. In these cases, we will ask that photos or videos with other pupils are not shared publicly on social media for safeguarding reasons, unless all the relevant parents/carers have agreed to this.

Where the school takes photographs and videos, 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.

When using photographs and videos in this way we will not accompany them with any other personal information about the child, to ensure they cannot be identified.

10. Artificial Intelligence (AI)

Artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Bard.

Fred Nicholson School recognises that AI has many uses to help pupils learn, but also poses risks to sensitive and personal data.

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

If personal and/or sensitive data is entered into an unauthorised generative AI tool, the school will treat this as a data breach, and will follow the personal data breach procedure outlined in appendix 1.

11. Data protection by design and default

We will 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 data 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 (see section 6)
- Completing data protection impact assessments where the school's processing of personal data 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 including this policy, 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
- Appropriate safeguards being put in place if we transfer any personal data outside of the UK, where different data protection laws may apply
- 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 data (via our privacy notices)

- For all personal data that we hold, maintaining an internal record of the type of data, type of data subject, how and why we are using the data, any third-party recipients, any transfers outside of the UK and the safeguards for those, retention periods and how we are keeping the data secure

11.1 Data security and storage of records

We will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage. In particular:

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data, are kept under lock and key when not in use
- Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, or left anywhere else where there is general access
- Where personal information needs to be taken off site, staff must sign it in and out from the school office
- Passwords that are at least 10 characters long containing letters and numbers are used to access school computers, laptops and other electronic devices. Staff and pupils are reminded that they should not reuse passwords from other sites
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices
- Staff, pupils or governors who store personal information on their personal devices are expected to follow the same security procedures as for school-owned equipment (see our E-safety policy/ICT policy/ Social Media & Electronic Communication Policy)
- Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected (see section 8)

11.2 Disposal of records

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it.

For example, we will shred or incinerate paper-based records, and overwrite or delete electronic files. We may also use a third party to safely dispose of records 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.

See **Annexe C** for full **Retention Schedule.**

12. Personal data breaches

In the case of a personal data breach, The School shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the Information Commissioner's Office, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons.

Where the notification to the Information Commissioner's Office is not made within 72 hours, it shall be accompanied by reasons for the delay.

In order to evaluate the personal data breach The School shall inform and involve the Data Protection Officer in the assessment of the breach and in the execution of the data breach procedure to contain and manage the breach.

The notification shall at least:

- describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
- communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;
- describe the likely consequences of the personal data breach;
- describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects;
- Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.

The School shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken in a data breach log. The log shall enable the Information Commissioner's Officer to verify compliance with the data breach rules and raise awareness of minor breaches that may assist in the identification of new data handling processes and training requirements.

Such breaches in a school context may include, but are not limited to:

12.1 Examples of data breaches

- Loss or theft of paper records or loss or theft of equipment on which data is stored e.g. a laptop, mobile phone, tablet device or memory stick;
- A letter or email containing personal and/or confidential data sent to the wrong

address (including internal staff or third parties) or an email to an unauthorised group of email boxes;

- Personal data disclosed orally in error in a meeting or over the phone – including "blogging" where information is obtained by deceiving The School, or where information has been disclosed without confirming the true identity of the requester;
- Unauthorised access to information classified as personal or confidential e.g. attaching documents to an outlook diary appointment that is openly accessible;
- Posting information on the world wide web or on a computer otherwise accessible from the Internet without proper information security precautions;
- Sensitive information left on a photo-copier or on a desk in County Council premises;
- Unauthorised alteration or deletion of information;
- Not storing personal and confidential information securely;
- Not ensuring the proper transfer or destruction of files after closure of offices/buildings e.g. not following building decommissioning procedures;
- Failure to safeguard/remove personal data on office equipment (including computers and smart phones) before disposal/sale.

12.2 Breaches caused by IT Security Incidents

Examples:

- Unauthorised access to IT systems because of misconfigured and/or inappropriate access controls;
- Hacking or phishing attacks and related suspicious activity;
- Virus or malware attacks and related suspicious activity;
- ICT infrastructure-generated suspicious activity;
- Divulging a password to another user without authority.

See **Appendix D** for details of a **personal data breach procedure** & Actions to **minimise the impact of data breaches**

13. Training

All staff and governors are provided with data protection training as part of their induction process.
Data protection will also form part of continuing professional development, where changes to legislation, guidance or the school's processes make it necessary.

20. Monitoring arrangements

The DPO is responsible for monitoring and reviewing this policy.
This policy will be reviewed annually and approved by the full governing board as recommended by the DfE.

Link to other Policies:

- GDPR Employee HR Data Policy
- Social Media & Electronic Communication Policy

Note: the annual review frequency here reflects the Department for Education's recommendation in its advice on statutory policies. This document has now been withdrawn, however the DfE's latest guidance does not include data protection in its list of statutory policies for maintained schools or academies, including free schools, however it is a legal requirement that the school has data protection policies and procedures in place.

Equality Impact Statement

We have carefully considered and analysed the impact of this policy on equality and the possible implications for pupils with protected characteristics, as part of our commitment to meet the Public Sector Equality Duty (PSED) requirement to have due regard to the need to eliminate discrimination, advance equality of opportunity and foster good relations.

Policy Approved by:

Hilary Bradshaw
Chair of Governors

Date: 2nd October 2024

Table of Changes		
29.10.23	2. Definitions	Confirmation of registration with ICO
	8. CCTV	Change of role to Premises Manager
	10. Artificial Intelligence	Addition of section - Artificial Intelligence. Following section numbers adjusted accordingly
	Link to Policies	Change of Policy from Internet, Social Networking and EMail Use Policy to Social Media & Electronic Communication Policy
	Equality Impact Statement	New proposed wording added

APPENDIX A –DEFINITIONS – this includes the information in the section above as well as other additional definitions that may be encountered

As defined by the UK GDPR:

- **personal data** means any information relating to an identified or identifiable natural person in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or by one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;
- **Data controller** means 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. Our school processes personal data of parents, pupils, staff, governors, visitors and others, and therefore, is a data controller.
- **data subject** means the identified or identifiable individual whose personal data is held or processed.
- **Data processing** means any operation or set of operations which is performed on personal data or on sets of personal data, automated or manual, such as collection, recording, School, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

- **restriction of processing** means the marking of stored personal data with the aim of limiting their processing in the future;
- **profiling** means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;
- **pseudonymisation** means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and Schoolal measures to ensure that the personal data are not attributed to an identified or identifiable natural person;
- **filing system** means 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 processor** means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;
- **Data recipient** means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance UK GDPR law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing;
- **third party** means 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;
- **consent** of the data subject 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 relating to him or her;
- **personal data breach** means 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;
- **genetic data** means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question;
- **biometric data** means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data;

- **data concerning health** means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status;
- **enterprise** means a natural or legal person engaged in an economic activity, irrespective of its legal form, including partnerships or associations regularly engaged in an economic activity;
- **supervisory authority** means an independent public authority which is established by the UK GDPR ;
- **relevant and reasoned objection** means an objection to a draft decision as to whether there is an infringement of this Regulation, or whether envisaged action in relation to the controller or processor complies with this Regulation, which clearly demonstrates the significance of the risks posed by the draft decision as regards the fundamental rights and freedoms of data subjects and, where applicable, the free flow of personal data within the Union;
- **information society service** means any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services;
- **international School** means an School and its subordinate bodies governed by public international law, or any other body which is set up by, or on the basis of, an agreement between two or more countries;
- **special categories** of personal data means personal data:
    - revealing racial or ethnic origin,
    - revealing political opinions,
    - revealing religious or philosophical beliefs or trade union membership,
    - the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person,
    - data concerning health (physical or mental) or data concerning a natural person's sex life or sexual orientation shall be prohibited;
- **data breach**: an incident or event in which personal and/or confidential data:
    - has potentially been viewed or used by an individual unauthorised to do so;
    - has had its integrity compromised;
    - is lost or is unavailable for a significant period.

Appendix B: DPO Job Description

FRED NICHOLSON SCHOOL

ADDITIONAL RESPONSIBILITIES WITHIN AN EXISTING ROLE

Area of Specialism:	Data Protection Officer
Attached to Post:	School Business Manager
Reporting to:	Head Teacher / Governing Body
Responsible for:	The DPO is responsible for ensuring and monitoring compliance with current data protection law, and has the knowledge, support and authority to do so effectively. They oversee the school's data protection processes, advise the school on best practice and ensure the all staff within the school are aware of their data protection responsibilities. Also responsible for managing data subject access requests and point of contact for the ICO and individuals whose data is processed by the school. Ensure data protection by design is embedded into school culture, including assisting and advising on undertaking data protection impact assessments, where necessary.
Context	This role is to take responsibility for data protection across the school, increase understanding with the business of Data Protection, drive best practice and ensure compliance.

Accountability

* Understand the schools' data processing activities, including the systems and procedures used and the data security involved.
* Ensure the school's overall compliance with data protection law by implementing appropriate technical and Schoolal measures.
* Prioritise the high-risk data processing areas and focus on compliance within these (ensure lower risk data processing remains compliant).
* Ensure the school has a data protection policy and keep this up to date.
* Be the schools point of contact for and manage:

- Data protection queries from staff, advising on obligations and issuing recommendations
- data subject access requests and individual queries regarding how an individual's personal data is used and their individual rights.
- the ICO in terms of requests for documentation, potential breaches, complaints and for seeking advice on data protection issues

* Maintain a data activities register of all data activities (for schools of 250+ employees) schools with less should maintain a data register for high-risk processing activities).
* Maintain a breach register and ensure staff understand what and how to report.
* Undertake internal audits of processing activities, to identify high risk areas and to make improvements where required.
* Ensure contracts with third party suppliers are compliant with data protection law in terms of data sharing. Work with these suppliers to ensure compliance.
* Ensure staff are data protection trained and provide updated or refresher training at appropriate intervals.
* Liaise with HR, ICT and Legal providers to ensure compliance with data protection law.
* Embed data protection by design into the culture of the school, using impact assessments where necessary and implementing measures to ensure only necessary data is processed.
* Report to and provide comprehensive reports to senior leaders and Governors/Trustees on the school's compliance, associated risks and advise on strategies.
* Be the school's data protection expert by maintaining and continually improving knowledge of data protection law, emerging security trends and security enhancing technology.
* Provide input into the wider developments of the information governance strategy and business planning process.
* Undertake any other tasks, as necessary to keep the school compliant with data protection law.
* Provide input into the wider developments of the information governance strategy and business planning process.
* Undertake any other tasks, as necessary to keep the school compliant with data protection law.

General information

* The job description details the main outcomes of the job and will be updated if these outcomes change.
* All work performed/duties undertaken must be carried out in accordance with relevant School policies and procedures, within legislation, and with regard to the needs of our customers and the diverse community we serve.

Job holders will be expected to be flexible in their duties and carry out any other duties commensurate with the grade and falling within the general scope of the job, as requested by management.

Appendix C Retention Schedule.

Contents

A. Aims

This checklist has been produced based on the "Information Management Toolkit for Schools" (IMTIS) dated 1 February 2016 and developed and published by the Information Record Management Society ("IRMS").

This checklist has been produced in accordance with the guidance produced by the DFE in April 2018 in the "GDPR Toolkit for Schools" and is in accordance with the Data Protection rules and Freedom of Information Act (2000) legislation.

This is a checklist developed to enable School Business Manager and other School Staff to carry out an efficient annual review and safe destruction of school records and information.

Where there is legal statute behind a requirement this is detailed in the IMTIS document.

B. Safe Destruction of Data

(i) Disposal of records that have reached the end of the minimum retention period allocated

The fifth data protection principle as per the data protection rules (updated for GDPR) states that:

"Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes"

In each school, the leadership must ensure that records that are no longer required for business use are reviewed as soon as possible under the criteria set out so that only the appropriate records are destroyed.

The school review will determine whether records are to be selected for permanent preservation, destroyed, digitised to an electronic format or retained by the school for research or litigation purposes.

Whatever decisions are made they need to be documented as part of the records management policy within the school.

(ii) Safe destruction of records

All records containing personal information, or sensitive policy information should be made either unreadable or unreconstructable.

- Paper records should be shredded using a cross-cutting shredder
- CDs / DVDs / Floppy Disks should be cut into pieces
- Audio / Video Tapes and Fax Rolls should be dismantled and shredded
- Hard Disks should be dismantled and sanded

Any other records should be bundled up and disposed of to a waste paper merchant or disposed of in other appropriate ways. Do not put records in with the regular waste or a skip unless there is no other alternative.

There are companies who can provide confidential waste bins and other services which can be purchased to ensure that records are disposed of in an appropriate way.

a) Where an external provider is used it is recommended that all records must be shredded on-site in the presence of an employee. The organisation must also be able to prove that the records have been destroyed by the company who should provide a Certificate of Destruction. Staff working for the external provider should have been trained in the handling of confidential documents.

   The shredding needs to be planned with specific dates and all records should be identified as to the date of destruction.

   It is important to understand that if the records are recorded as to be destroyed but have not yet been destroyed and a request for the records has been received they MUST still be provided.

b) Where records are destroyed internally, the process must ensure that all records are recorded are authorised to be destroyed by a member of the Leadership team and the destruction recorded. Records should be shredded as soon as the record has been documented as being destroyed.

(iii) Freedom of Information Act 2000 (FoIA 2000)

The Freedom of Information Act 2000 requires the school to maintain a list of records which have been destroyed and who authorised their destruction

Members of staff should record at least:

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

Following this guidance will ensure that the school is compliant with the Data Protection rules and the Freedom of Information Act 2000.

1. Management of the School

This section contains retention periods connected to the general management of the school. This covers the work of the Governing Body, the Headteacher and the senior management team, the admissions process and operational administration.

1.1 Governing Body					
Ref	**Basic file description**	**Data Protection Issues**	**Retention Period [Operational]**	**Action at the end of the administrative life of the record**	**Annual Review Completed Tick (√)**
1.1.1	Agendas for Governing Body meetings	There may be data protection issues if the meeting is dealing with confidential issues relating to staff	One copy should be retained with the master set of minutes. All other copies can be disposed of	SECURE DISPOSAL[1]	
1.1.2	Minutes of Governing Body meetings	There may be data protection issues if the meeting is dealing with confidential issues relating to staff			
	Principal Set (signed)		PERMANENT	If the school is unable to store these then they should be offered to the County Archives Service	
	Inspection Copies[2]		Date of meeting + 3 years	If these minutes contain any sensitive, personal information they must be shredded.	
1.1.3	Reports presented to the Governing Body	There may be data protection issues if the report deals with confidential issues relating to staff	Reports should be kept for a minimum of 6 years. However, if the minutes refer directly to individual reports then the reports should be kept permanently	SECURE DISPOSAL or retain with the signed set of the minutes	

[1] In this context SECURE DISPOSAL should be taken to mean disposal using confidential waste bins, or if the school has the facility, shredding using a cross cut shredder.

[2] These are the copies which the clerk to the Governor may wish to retain so that requestors can view all the appropriate information without the clerk needing to print off and collate redacted copies of the minutes each time a request is made.

1.1.4	Meeting papers relating to the annual parents' meeting held under section 33 of the Education Act 2002	No	Date of the meeting + a minimum of 6 years	SECURE DISPOSAL	

1.1 Governing Body (continued…)					
Ref	**Basic file description**	**Data Protection Issues**	**Retention Period [Operational]**	**Action at the end of the administrative life of the record**	**Annual Review Completed Tick (√)**
1.1.5	Instruments of Government including Articles of Association	No	PERMANENT	These should be retained in the school whilst the school is open and then offered to County Archives Service when the school closes.	
1.1.6	Trusts and Endowments managed by the Governing Body	No	PERMANENT	These should be retained in the school whilst the school is open and then offered to County Archives Service when the school closes.	
1.1.7	Action plans created and administered by the Governing Body	No	Life of the action plan + 3 years	SECURE DISPOSAL	
1.1.8	Policy documents created and administered by the Governing Body	No	Life of the policy + 3 years	SECURE DISPOSAL	
1.1.9	Records relating to complaints dealt with by the Governing Body	Yes	Date of the resolution of the complaint + a minimum of 6 years then review for further retention in case of contentious disputes	SECURE DISPOSAL	
1.1.10	Annual Reports created under the requirements of the Education (Governor's Annual Reports) (England) (Amendment) Regulations 2002	No	Date of report + 10 years	SECURE DISPOSAL	

1.1.11	Proposals concerning the change of status of a maintained school including Specialist Status Schools and Academies	No	Date proposal accepted or declined + 3 years	SECURE DISPOSAL	

1.2 Head Teacher and Senior Management Team					
Ref	**Basic file description**	**Data Protection Issues**	**Retention Period [Operational]**	**Action at the end of the administrative life of the record**	**Annual Review Completed Tick (√)**
1.2.1	Log books of activity in the school maintained by the Head Teacher	There may be data protection issues if the log book refers to individual pupils or members of staff	Date of last entry in the book + a minimum of 6 years then review	These could be of permanent historical value and should be offered to the County Archives Service if appropriate	
1.2.2	Minutes of Senior Management Team meetings and the meetings of other internal administrative bodies	There may be data protection issues if the minutes refers to individual pupils or members of staff	Date of the meeting + 3 years then review	SECURE DISPOSAL	
1.2.3	Reports created by the Head Teacher or the Management Team	There may be data protection issues if the report refers to individual pupils or members of staff	Date of the report + a minimum of 3 years then review	SECURE DISPOSAL	
1.2.4	Records created by head teachers, deputy head teachers, heads of year and other members of staff with administrative responsibilities	There may be data protection issues if the records refer to individual pupils or members of staff	Current academic year + 6 years then review	SECURE DISPOSAL	

1.2.5	Correspondence created by head teachers, deputy head teachers, heads of year and other members of staff with administrative responsibilities	There may be data protection issues if the correspondence refers to individual pupils or members of staff	Date of correspondence + 3 years then review	SECURE DISPOSAL	
1.2.6	Professional Development Plans	Yes	Life of the plan + 6 years	SECURE DISPOSAL	
1.2.7	School Development Plans	No	Life of the plan + 3 years	SECURE DISPOSAL	

1.3 Admissions Process					
Ref	**Basic file description**	**Data Protection Issues**	**Retention Period [Operational]**	**Action at the end of the administrative life of the record**	**Annual Review Completed Tick (√)**
1.3.1	All records relating to the creation and implementation of the School Admissions' Policy	No	Life of the policy + 3 years then review	SECURE DISPOSAL	
1.3.2	Admissions – if the admission is successful	Yes	Date of admission + 1 year	SECURE DISPOSAL	
1.3.3	Admissions – if the appeal is unsuccessful	Yes	Resolution of case + 1 year	SECURE DISPOSAL	
1.3.4	Register of Admissions	Yes	Every entry in the admission register must be preserved for a period of three years after the date on which the entry was made.[3]	REVIEW Schools may wish to consider keeping the admission register permanently as often schools receive enquiries from past pupils to confirm the dates they attended the school.	
1.3.5	Admissions – Secondary Schools – Casual	Yes	Current year + 1 year	SECURE DISPOSAL	
1.3.6	Proofs of address supplied by parents as part of the admissions process	Yes	Current year + 1 year	SECURE DISPOSAL	

1.3.7	Supplementary Information form including additional information such as religion, medical conditions etc	Yes			
	For successful admissions		This information should be added to the pupil file	SECURE DISPOSAL	
	For unsuccessful admissions		Until appeals process completed	SECURE DISPOSAL	

1.4 Operational Administration					
Ref	**Basic file description**	**Data Protection Issues**	**Retention Period [Operational]**	**Action at the end of the administrative life of the record**	**Annual Review Completed Tick (√)**
1.4.1	General file series	No	Current year + 5 years then REVIEW	SECURE DISPOSAL	
1.4.2	Records relating to the creation and publication of the school brochure or prospectus	No	Current year + 3 years	STANDARD DISPOSAL	
1.4.3	Records relating to the creation and distribution of circulars to staff, parents or pupils	No	Current year + 1 year	STANDARD DISPOSAL	
1.4.4	Newsletters and other items with a short operational use	No	Current year + 1 year	STANDARD DISPOSAL	
1.4.5	Visitors' Books and Signing in Sheets	Yes	Current year + 6 years then REVIEW	SECURE DISPOSAL	
1.4.6	Records relating to the creation and management of Parent Teacher Associations and/or Old Pupils Associations	No	Current year + 6 years then REVIEW	SECURE DISPOSAL	

2. Human Resources

This section deals with all matters of Human Resources management within the school.

2.1 Recruitment					
Ref	**Basic file description**	**Data Protection Issues**	**Retention Period [Operational]**	**Action at the end of the administrative life of the record**	**Annual Review Completed Tick (√)**
2.1.1	All records leading up to the appointment of a new headteacher	Yes	Date of appointment + 6 years	SECURE DISPOSAL	
2.1.2	All records leading up to the appointment of a new member of staff – unsuccessful candidates	Yes	Date of appointment of successful candidate + 6 months	SECURE DISPOSAL	
2.13	All records leading up to the appointment of a new member of staff – successful candidate	Yes	All the relevant information should be added to the staff personal file (see below) and all other information retained for 6 months	SECURE DISPOSAL	
2.1.4	Pre-employment vetting information – DBS Checks	No	The school does not have to keep copies of DBS certificates. If the school does so the copy must NOT be retained for more than 6 months		
2.1.5	Proofs of identity collected as part of the process of checking "portable" enhanced DBS disclosure	Yes	Where possible these should be checked and a note kept of what was seen and what has been checked. If it is felt necessary to keep copy documentation then this should be placed on the member of staff's personal file		

2.1.6	Pre-employment vetting information – Evidence proving the right to work in the United Kingdom[4]	Yes	Where possible these documents should be added to the Staff Personal File [see below], but if they are kept separately then the Home Office requires that the documents are kept for termination of Employment plus not less than two years		

2.2 Operational Staff Management					
Ref	**Basic file description**	**Data Protection Issues**	**Retention Period [Operational]**	**Action at the end of the administrative life of the record**	**Annual Review Completed Tick (√)**
2.2.1	Staff Personal File	Yes	Termination of Employment + 6 years	SECURE DISPOSAL	
2.2.2	Timesheets	Yes	Current year + 6 years	SECURE DISPOSAL	
2.2.3	Annual appraisal/ assessment records	Yes	Current year + 5 years	SECURE DISPOSAL	

2.3 Management of Disciplinary and Grievance Processes					
Ref	**Basic file description**	**Data Protection Issues**	**Retention Period [Operational]**	**Action at the end of the administrative life of the record**	**Annual Review Completed Tick (√)**
2.3.1	Allegation of a child protection nature against a member of staff including where the allegation is unfounded[5]	Yes	Until the person's normal retirement age or 10 years from the date of the allegation whichever is the longer then REVIEW. Note allegations that are found to be malicious should be removed from personnel files. If found they are to be kept on the file and a copy provided to the person concerned	SECURE DISPOSAL These records must be shredded	
2.3.2	Disciplinary Proceedings	Yes			

	oral warning		Date of warning + 6 months	SECURE DISPOSAL [If warnings are placed on personal files then they must be weeded from the file]	
	written warning – level 1		Date of warning + 6 months		
	written warning – level 2		Date of warning + 12 months		
	final warning		Date of warning + 18 months		
	case not found		If the incident is child protection related then see above otherwise dispose of at the conclusion of the case	SECURE DISPOSAL	

2.4 Health and Safety					
Ref	**Basic file description**	**Data Protection Issues**	**Retention Period [Operational]**	**Action at the end of the administrative life of the record**	**Annual Review Completed Tick (√)**
2.4.1	Health and Safety Policy Statements	No	Life of policy + 3 years	SECURE DISPOSAL	
2.4.2	Health and Safety Risk Assessments	No	Life of risk assessment + 3 years	SECURE DISPOSAL	
2.4.3	Records relating to accident/ injury at work	Yes	Date of incident + 12 years In the case of serious accidents a further retention period will need to be applied	SECURE DISPOSAL	
2.4.4	Accident Reporting	Yes			
	Adults		Date of the incident + 6 years	SECURE DISPOSAL	
	Children		DOB of the child + 25 years	SECURE DISPOSAL	
2.4.5	Control of Substances Hazardous to Health (COSHH)	No	Current year + 40 years	SECURE DISPOSAL	
2.4.6	Process of monitoring of areas where employees and persons are likely to have become in contact with asbestos	No	Last action + 40 years	SECURE DISPOSAL	
2.4.7	Process of monitoring of areas where employees and persons are likely to have become in contact with radiation	No	Last action + 50 years	SECURE DISPOSAL	
2.4.8	Fire Precautions log books	No	Current year + 6 years	SECURE DISPOSAL	

2.4 Payroll and Pensions

Ref	Basic file description	Data Protection Issues	Retention Period [Operational]	Action at the end of the administrative life of the record	Annual Review Completed Tick (√)
2.5.1	Maternity pay records	Yes	Current year + 3 years	SECURE DISPOSAL	
2.5.2	Records held under Retirement Benefits Schemes (Information Powers) Regulations 1995	Yes	Current year + 6 years	SECURE DISPOSAL	

3. Financial Management of the School

This section deals with all aspects of the financial management of the school including the administration of school meals

3.1 Risk Management and Insurance					
Ref	**Basic file description**	**Data Protection Issues**	**Retention Period [Operational]**	**Action at the end of the administrative life of the record**	**Annual Review Completed Tick (√)**
3.1.1	Employer's Liability Insurance Certificate	No	Closure of the school + 40 years	SECURE DISPOSAL	

3.2 Asset Management					
Ref	**Basic file description**	**Data Protection Issues**	**Retention Period [Operational]**	**Action at the end of the administrative life of the record**	**Annual Review Completed Tick (√)**
3.2.1	Inventories of furniture and equipment	No	Current year + 6 years	SECURE DISPOSAL	
3.2.2	Burglary, theft and vandalism report forms	No	Current year + 6 years	SECURE DISPOSAL	

3.3 Accounts and Statements including Budget Management					
Ref	**Basic file description**	**Data Protection Issues**	**Retention Period [Operational]**	**Action at the end of the administrative life of the record**	**Annual Review Completed Tick (√)**
3.3.1	Annual Accounts	No	Current year + 6 years	STANDARD DISPOSAL	
3.3.2	Loans and grants managed by the school	No	Date of last payment on the loan + 12 years then REVIEW	SECURE DISPOSAL	
3.3.3	Student Grant applications	Yes	Current year + 3 years	SECURE DISPOSAL	

3.3.4	All records relating to the creation and management of budgets including the Annual Budget statement and background papers	No	Life of the budget + 3 years	SECURE DISPOSAL	
3.3.5	Invoices, receipts, order books and requisitions, delivery notices	No	Current financial year + 6 years	SECURE DISPOSAL	
3.3.6	Records relating to the collection and banking of monies	No	Current financial year + 6 years	SECURE DISPOSAL	
3.3.7	Records relating to the identification and collection of debt	No	Current financial year + 6 years	SECURE DISPOSAL	

3.4 Contract Management					
Ref	**Basic file description**	**Data Protection Issues**	**Retention Period [Operational]**	**Action at the end of the administrative life of the record**	**Annual Review Completed Tick (√)**
3.4.1	All records relating to the management of contracts under seal	No	Last payment on the contract + 12 years	SECURE DISPOSAL	
3.4.2	All records relating to the management of contracts under signature	No	Last payment on the contract + 6 years	SECURE DISPOSAL	
3.4.3	Records relating to the monitoring of contracts	No	Current year + 2 years	SECURE DISPOSAL	

3.5 School Fund					
Ref	**Basic file description**	**Data Protection Issues**	**Retention Period [Operational]**	**Action at the end of the administrative life of the record**	**Annual Review Completed Tick (√)**
3.5.1	School Fund - Cheque books	No	Current year + 6 years	SECURE DISPOSAL	

3.5.2	School Fund - Paying in books	No	Current year + 6 years	SECURE DISPOSAL	
3.5.3	School Fund – Ledger	No	Current year + 6 years	SECURE DISPOSAL	N/A
3.5.4	School Fund – Invoices	No	Current year + 6 years	SECURE DISPOSAL	
3.5.5	School Fund – Receipts	No	Current year + 6 years	SECURE DISPOSAL	
3.5.6	School Fund - Bank statements	No	Current year + 6 years	SECURE DISPOSAL	
3.5.7	School Fund – Journey Books	No	Current year + 6 years	SECURE DISPOSAL	N/A

3.6 School Meals					
Ref	**Basic file description**	**Data Protection Issues**	**Retention Period [Operational]**	**Action at the end of the administrative life of the record**	**Annual Review Completed Tick (√)**
3.6.1	Free School Meals Registers	Yes	Current year + 6 years	SECURE DISPOSAL	
3.6.2	School Meals Registers	Yes	Current year + 3 years	SECURE DISPOSAL	
3.6.3	School Meals Summary Sheets	No	Current year + 3 years	SECURE DISPOSAL	

4. Property Management

This section covers the management of buildings and property.

4.1 Property Management					
Ref	**Basic file description**	**Data Protection Issues**	**Retention Period [Operational]**	**Action at the end of the administrative life of the record**	**Annual Review Completed Tick (√)**

4.1.1	Title deeds of properties belonging to the school	No	PERMANENT These should follow the property unless the property has been registered with the Land Registry		
4.1.2	Plans of property belong to the school	No	These should be retained whilst the building belongs to the school and should be passed onto any new owners if the building is leased or sold.		
4.1.3	Leases of property leased by or to the school	No	Expiry of lease + 6 years	SECURE DISPOSAL	
4.1.4	Records relating to the letting of school premises	No	Current financial year + 6 years	SECURE DISPOSAL	

4.2 Maintenance					
Ref	**Basic file description**	**Data Protection Issues**	**Retention Period [Operational]**	**Action at the end of the administrative life of the record**	**Annual Review Completed Tick (√)**
4.2.1	All records relating to the maintenance of the school carried out by contractors	No	Current year + 6 years	SECURE DISPOSAL	
4.2.2	All records relating to the maintenance of the school carried out by school employees including maintenance log books	No	Current year + 6 years	SECURE DISPOSAL	

5. Pupil Management

This section includes all records which are created during the time a pupil spends at the school. For information about accident reporting see under Health and Safety above

5.1 Pupil's Educational Record					
Ref	**Basic file description**	**Data Protection Issues**	**Retention Period [Operational]**	**Action at the end of the administrative life of the record**	**Annual Review Completed Tick (√)**
5.1.1	Pupil's Educational Record required by The Education (Pupil Information) (England) Regulations 2005	Yes			
	Primary		Retain whilst the child remains at the primary school	The file should follow the pupil when he/she leaves the primary school. [3]	
	Secondary		Date of Birth of the pupil + 25 years	SECURE DISPOSAL	
5.1.2	Examination Results – Pupil Copies	Yes			
	Public		This information should be added to the pupil file	All uncollected certificates should be returned to the examination board.	
	Internal		This information should be added to the pupil file		

[3] This will include: (i) to another primary school (ii) to a secondary school (iii) to a pupil referral unit (iv) If the pupil dies whilst at primary school the file should be returned to the Local Authority to be retained for the statutory retention period. If the pupil transfers to an independent school, transfers to home schooling or leaves the country the file should be returned to the Local Authority to be retained for the statutory retention period. Primary Schools do not ordinarily have sufficient storage space to store records for pupils who have not transferred in the normal way. It makes more sense to transfer the record to the Local Authority as it is more likely that the pupil will request the record from the Local Authority

5.1.3	Child Protection information held on pupil file		If any records relating to child protection issues are placed on the pupil file, it should be in a sealed envelope and then retained for the same period of time as the pupil file.	SECURE DISPOSAL – these records MUST be shredded	
5.1.4	Child protection information held in separate files		DOB of the child + 25 years then review This retention period was agreed in consultation with the Safeguarding Children Group on the understanding that the principal copy of this information will be found on the Local Authority Social Services record	SECURE DISPOSAL – these records MUST be shredded	

5.2 Attendance					
Ref	**Basic file description**	**Data Protection Issues**	**Retention Period [Operational]**	**Action at the end of the administrative life of the record**	**Annual Review Completed Tick (√)**
5.2.1	Attendance Registers	Yes	Every entry in the attendance register must be preserved for a period of three years after the date on which the entry was made.	SECURE DISPOSAL	
5.2.2	Correspondence relating to authorized absence		Current academic year + 2 years	SECURE DISPOSAL	

5.3 Special Educational Needs					
Ref	**Basic file description**	**Data Protection Issues**	**Retention Period [Operational]**	**Action at the end of the administrative life of the record**	**Annual Review Completed Tick (√)**

5.3.1	Special Educational Needs files, reviews and Individual Education Plans	Yes	Date of Birth of the pupil + 25 years	REVIEW NOTE: This retention period is the minimum retention period that any pupil file should be kept. Some authorities choose to keep SEN files for a longer period of time to defend themselves in a “failure to provide a sufficient education” case. There is an element of business risk analysis involved in any decision to keep the records longer than the minimum retention period and this should be documented.	
5.3.2	Statement maintained under section 234 of the Education Act 1990 and any amendments made to the statement	Yes	Date of birth of the pupil + 25 years [This would normally be retained on the pupil file]	SECURE DISPOSAL unless the document is subject to a legal hold	
			Date of birth of the pupil + 25 years [This would normally be retained on the pupil file]	SECURE DISPOSAL unless the document is subject to a legal hold	

			Date of birth of the pupil + 25 years [This would normally be retained on the pupil file]	SECURE DISPOSAL unless the document is subject to a legal hold	

6. Curriculum Management

6.1 Statistics and Management Information					
Ref	**Basic file description**	**Data Protection Issues**	**Retention Period [Operational]**	**Action at the end of the administrative life of the record**	**Annual Review Completed Tick (√)**
6.1.1	Curriculum returns	No	Current year + 3 years	SECURE DISPOSAL	
6.1.2	Examination Results (Schools Copy)	Yes	Current year + 6 years	SECURE DISPOSAL	
	SATS records –	Yes			
	Results		The SATS results should be recorded on the pupil's educational file and will therefore be retained until the pupil reaches the age of 25 years. The school may wish to keep a composite record of all the whole year SATs results. These could be kept for current year + 6 years to allow suitable comparison	SECURE DISPOSAL	
	Examination Papers		The examination papers should be kept until any appeals/validation process is complete	SECURE DISPOSAL	
6.1.3	Published Admission Number (PAN) Reports	Yes	Current year + 6 years	SECURE DISPOSAL	
6.1.4	Value Added and Contextual Data	Yes	Current year + 6 years	SECURE DISPOSAL	
6.1.5	Self-Evaluation Forms	Yes	Current year + 6 years	SECURE DISPOSAL	

6.2 Implementation of Curriculum					
Ref	**Basic file description**	**Data Protection Issues**	**Retention Period [Operational]**	**Action at the end of the administrative life of the record**	**Annual Review Completed Tick (√)**

6.2.1	Schemes of Work	No	Current year + 1 year	Review these records at the end of each year and allocate a further retention period or SECURE DISPOSAL	
6.2.2	Timetable	No	Current year + 1 year		
6.2.3	Class Record Books	No	Current year + 1 year		
6.2.4	Mark Books	No	Current year + 1 year		
6.2.5	Record homework set	No	Current year + 1 year		
6.2.6	Pupils' Work	No	Where possible pupils' work should be returned to the pupil at the end of the academic year if this is not the school's policy then current year + 1 year	SECURE DISPOSAL	

7. Extra Curriculum Management

7.1 Educational Visits outside the Classroom					
Ref	**Basic file description**	**Data Protection Issues**	**Retention Period [Operational]**	**Action at the end of the administrative life of the record**	**Annual Review Completed Tick (√)**
7.1.1	Records created by schools to obtain approval to run an Educational Visit outside the Classroom – Primary Schools	No	Date of visit + 14 years	SECURE DISPOSAL	
7.1.2	Records created by schools to obtain approval to run an Educational Visit outside the Classroom – Secondary Schools	No	Date of visit + 10 years	SECURE DISPOSAL	

7.1.3	Parental consent forms for school trips where there has been no major incident	Yes	Conclusion of the trip	Although the consent forms could be retained for DOB + 22 years, the requirement for them being needed is low and most schools do not have the storage capacity to retain every single consent form issued by the school for this period of time.	
7.1.4	Parental permission slips for school trips – where there has been a major incident	Yes	DOB of the pupil involved in the incident + 25 years The permission slips for all the pupils on the trip need to be retained to show that the rules had been followed for all pupils		

7.3 Family Liaison Officers and Home School Liaison Assistants					
Ref	**Basic file description**	**Data Protection Issues**	**Retention Period [Operational]**	**Action at the end of the administrative life of the record**	**Annual Review Completed Tick (√)**
7.3.1	Day Books	Yes	Current year + 2 years then review		
7.3.2	Reports for outside agencies - where the report has been included on the case file created by the outside agency	Yes	Whilst child is attending school and then destroy		
7.3.3	Referral forms	Yes	While the referral is current		
7.3.4	Contact data sheets	Yes	Current year then review, if contact is no longer active then destroy		

7.3.5	Contact database entries	Yes	Current year then review, if contact is no longer active then destroy		
7.3.6	Group Registers	Yes	Current year + 2 years		

8. Central Government and Local Authority

8.1 Local Authority					
Ref	**Basic file description**	**Data Protection Issues**	**Retention Period [Operational]**	**Action at the end of the administrative life of the record**	**Annual Review Completed Tick (√)**
8.1.1	Secondary Transfer Sheets (Primary)	Yes	Current year + 2 years	SECURE DISPOSAL	
8.1.2	Attendance Returns	Yes	Current year + 1 year	SECURE DISPOSAL	
8.1.3	School Census Returns	No	Current year + 5 years	SECURE DISPOSAL	
8.1.4	Circulars and other information sent from the Local Authority	No	Operational use	SECURE DISPOSAL	

8.2 Central Government					
Ref	**Basic file description**	**Data Protection Issues**	**Retention Period [Operational]**	**Action at the end of the administrative life of the record**	**Annual Review Completed Tick (√)**
8.2.1	OFSTED reports and papers	No	Life of the report then REVIEW	SECURE DISPOSAL	
8.2.2	Returns made to central government	No	Current year + 6 years	SECURE DISPOSAL	
8.2.3	Circulars and other information sent from central government	No	Operational use	SECURE DISPOSAL	

Appendix C(i) – List of School Records and Data safely destroyed

The following sheet can be completed or alternatively documented in a spreadsheet.

Ref Number	File/Record Title	Description	Reference or Cataloguing Information	Number of Files Destroyed	Method of destruction	Confirm (i) Safely destroyed (ii) In accordance with Data Retention Guidelines Tick (√)
e.g.	*School Invoices*	*Copies of purchase invoices dated 2011/12*	*Folders marked "Purchase Invoices 2011/12" 1 to 3*	*3 Folders*	*Shredding*	√
1						
2						
3						
4						
5						
6						
7						
8						
9						
10						
11						
12						

Ref Number	File/Record Title	Description	Reference or Cataloguing Information	Number of Files Destroyed	Method of destruction	Confirm (i) Safely destroyed (ii) In accordance with Data Retention Guidelines Tick (√)
13						
14						

Appendix D: Personal data breach procedure & Actions to minimise the impact of data breaches

This procedure is based on guidance on personal data breaches produced by the Information Commissioner's Office (ICO).

- On finding or causing a breach, or potential breach, the staff member, governor or data processor must immediately notify the Data Protection Officer (DPO) by email which includes the date, time and content of the breach; who has received the data and how this has been shared e.g. letter, email; what action has been taken following discovery of the breach.
- Information will be shared with Data Protection Education with whom school has a subscription for specialist advice and support.
- The DPO, with the support of DPE, will investigate the report, and determine whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidentally or unlawfully:
    - Lost
    - Stolen
    - Destroyed
    - Altered
    - Disclosed or made available where it should not have been
    - Made available to unauthorised people
- Staff and governors will cooperate with the investigation (including allowing access to information and responding to questions). The investigation will not be treated as a disciplinary investigation.
- If a breach has occurred or it is considered to be likely that is the case, 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. Relevant staff members or data processors should help the DPO with this where necessary, and the DPO should take external advice when required (e.g. from IT providers). (See the actions relevant to specific data types at the end of this procedure)
- The DPO will assess the potential consequences (based on how serious they are and how likely they are to happen) before and after the implementation of steps to mitigate the consequences
- The DPO will take advice from DPE regarding whether the breach must be reported to the ICO and the individuals affected via the FNS area of the Data Protection Education website.
- The DPO will document the decisions (either way), in case the decisions are challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored on the FNS area of the Data Protection Education website.

Where the ICO must be notified, the DPO will do this with the support of Data Protection Education using the 'Report a breach' page of the ICO website, or through its breach report line (0303 123 1113), within 72 hours of the school's awareness of the breach. As required, the DPO will set out:

- A description of the nature of the personal data breach including, where possible:
    - The categories and approximate number of individuals concerned
    - The categories and approximate number of personal data records concerned
- The name and contact details of the DPO
- A description of the likely consequences of the personal data 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 of the school's awareness of the breach. 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
- Where the school is required to communicate with individuals whose personal data has been breached, the DPO will tell them in writing. This notification will set out:
    - A description, in clear and plain language, of the nature of the personal data breach
    - The name and contact details of the DPO
    - A description of the likely consequences of the personal data 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 consider, in light of the investigation and any engagement with affected individuals, whether to 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 the FNS area of the Data Protection Education website.

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

- The DPO and headteacher will meet as required to assess recorded data breaches and identify any trends or patterns requiring action by the school to reduce risks of future breaches

Actions to minimise the impact of data breaches

We set out below the steps we might take to try and mitigate the impact of different types of data breach if they were to occur, focusing especially on breaches involving particularly risky or sensitive information. We will review the effectiveness of these actions and amend them as necessary after any data breach.

Set out the relevant actions you will take for different types of risky or sensitive personal data processed by your school. For example:

Sensitive information being disclosed via email (including safeguarding records)

- If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error
- Members of staff who receive personal data sent in error must alert the sender and the DPO as soon as they become aware of the error
- If the sender is unavailable or cannot recall the email for any reason, the DPO will ask the [ICT department/external IT support provider] to attempt to recall it from external recipients and remove it from the school's email system (retaining a copy if required as evidence)
- In any cases where the recall is unsuccessful or cannot be confirmed as successful, the DPO will consider whether it's appropriate to contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way

- The DPO will endeavor to obtain a written response from all the individuals who received the data, confirming that they have complied with this request
- The DPO will carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted
- If safeguarding information is compromised, the DPO will inform the DSL and discuss whether the school should inform any, or all, of its 3 local safeguarding partners.

Other types of breach that you might want to consider could include:

- Details of pupil premium interventions for named children being published on the school website
- Non-anonymised pupil exam results or staff pay information being shared with governors
- A school laptop containing non-encrypted sensitive personal data being stolen or hacked
- The school's cashless payment provider being hacked and parents' financial details stolen
- Hardcopy reports sent to the wrong pupils or families