





## DATA PROTECTION POLICY

Formally adopted by the Governing Body of Sheringham Community Primary & Nursery School	
On	23 <sup>rd</sup> November 2023
Chair of Governors	
Head Teacher	
Last updated	23 <sup>rd</sup> November 2023
Review	23 <sup>rd</sup> November 2024

***Be all that you can be...***



## Contents

1. Commitment to General Data Protection and Data Protection by Design .....	3
2. Policy Objectives Roles Responsibilities .....	3
3. Policy Statement.....	4
4. About this Policy .....	4
5. Data Protection Officer .....	5
6. Data Protection Principles.....	6
7. Data Subject's Rights .....	7
8. Fair and Transparent Processing of Data .....	7
9. Lawful Processing of Data .....	9
10. Special Category Data .....	9
11. Consent.....	9
12. Disclosure and Sharing of Personal Information.....	11
13. Data Security.....	11
14. Data Protection Impact Assessments.....	12
15. Data Breaches .....	12
16. Subject Access Requests.....	13
17. Publication of Information.....	14
18. DBS Data.....	14
19. Photography Images and Videos.....	15
21. Retention Policy .....	16
22. Training.....	16
23. Data Processors .....	17
24. Changes to this Policy.....	17
Appendix 1: GDPR Definitions.....	18
Appendix 2: Examples of Data Breaches .....	21
Appendix 3: Dealing with Subject Access Requests .....	22
Appendix 4: Annual review of school records and safe data destruction checklist. .	24

## 1. Commitment to General Data Protection and Data Protection by Design

- 1.1 General Data Protection Regulation (GDPR) and The Data Protection Act 2018 (DPA) is the law that protects personal privacy and upholds individual's rights. It applies to anyone who handles or has access to people's personal data.
- 1.2 This policy is intended to ensure that personal information is dealt with properly and securely and in accordance with the legislation. It will apply to personal information regardless of the way it is used, recorded and stored and whether it is held in paper files or electronically.
- 1.3 This policy sets out the organisations commitment to GDPR and the implementation of a data protection by design approach.
- 1.4 The organisation will refer to documents and guidance from the Information Commissioner's Office and the Department for Education in relation to GDPR and data processing.
- 1.5 This includes ensuring the following:
  - The creation and maintenance of a data protection working group;
  - Assigning responsibility to an individual within The Organisation;
  - Assigning a Data Protection Officer;
  - Development and maintenance of a GDPR project;
  - Ensuring that all staff are trained in data protection and take responsibility for the collection, processing, storage and destruction of data;
  - A lawful basis for processing is documented for all processing activity;
  - Principles relating to processing of personal data are adhered to;
  - The rights of data subjects are respected;
  - Risks to the rights of data subjects are assessed and mitigated for all large-scale and new processing;
  - Regular independent reviews of processing activity and processing documentation are carried out;
  - Organisational and technical measures are implemented to protect data;
  - Data breaches impacting on the rights and freedoms of data subjects will be reported to the Information Commissioner's Office (ICO).

## 2. Policy Objectives Roles Responsibilities

- 2.1 **The organisation as the Data Controller** will comply with its obligations under the GDPR and the Data Protection Act 2018. The organisation is committed to being concise, clear and transparent about how it obtains and uses personal information and will ensure data subjects are aware of their rights under the legislation. This policy sets out how the organisation will do this.

- 2.2 All organisation staff and organisation workforce must have a general understanding of the law and understand how it may affect their decisions in order to make an informed judgement about how information is gathered, used and ultimately deleted. All staff must read, understand and comply with this policy in order to comply with its obligations under GDPR and the Data Protection Act 2018.
- 2.3 **The Information Commissioner as the Regulator** can impose substantial fines for breaches of GDPR and the Data Protection Act 2018 and other Data Protection Legislation. Therefore it is imperative that the organisation, all staff and the workforce comply with the legislation. The Data Protection Officer will be the principal point of contact with the ICO.

### 3. Policy Statement

- 3.1 Everyone has rights with regard to the way in which their personal data is handled. During the course of our activities as an organisation we will collect, store and process personal data about our pupils, workforce, parents and others. This makes us a data controller in relation to that personal data.
- 3.2 We are committed to the protection of all personal data and special category personal data for which we are the data controller.
- 3.3 The law imposes significant fines for failing to lawfully process and safeguard personal data and failure to comply with this policy may result in those fines being applied.
- 3.4 All members of our staff and workforce will comply with this policy when processing personal data on our behalf. Any breach of this policy may result in disciplinary or other action.

### 4. About this Policy

- 4.1 The types of personal data that we may be required to handle include information about pupils, parents, our workforce, and others that we deal with. The personal data which we hold is subject to certain legal safeguards specified in the General Data Protection Regulation the Data Protection Act 2018, and other regulations Data Protection Legislation
- 4.2 This policy does not form part of any employee's contract of employment and may be amended at any time.
- 4.3 This policy sets out rules on data protection and the legal conditions that must be satisfied when the organisation processes personal data.

- 4.4 This policy, combined with the organisations privacy policy and any other document referred to herein, sets out the basis on which the organisation will process any personal data collected from data subjects, or provided to us by data subjects directly and or from other sources.

## 5. Data Protection Officer

- 5.1 As a organisation we are required to appoint a Data Protection Officer ("DPO"). **Our DPO is Data Protection Education** and they can be contacted at [dpo@dataprotection.education](mailto:dpo@dataprotection.education)

The DPO is responsible for ensuring compliance with the Data Protection Legislation and with this policy. Any questions about the operation of this policy or any concerns that the policy has not been followed should be referred in the first instance to the DPO.

- 5.2 The organisation shall maintain a Data Protection Officer to represent the rights of data subjects and a named Data Protection lead in order to assist the Data Protection Officer.
- 5.3 The organisation shall ensure that the Data Protection Officer is involved properly and in a timely manner, in all issues which relate to the protection of personal data.
- 5.4 The organisation shall support the Data Protection Officer in performing the responsibilities outlined below by providing resources necessary to carry out those tasks and access to personal data and processing operations. The Data Protection Officer shall maintain his or her expert knowledge.
- 5.5 The organisation shall ensure that the Data Protection Officer 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.
- 5.6 The School Business Manager shall directly report to the highest management level of the organisation, as needed and report to the Board of Governors at least once a year.
- 5.7 Data subjects may contact the Data Protection Officer with regard to all issues related to processing of their personal data and to the exercise of their rights under the regulations.
- 5.8 The Data Protection Officer and the Data Protection Lead will be bound by confidentiality and must maintain data security by protecting the confidentiality, integrity and availability of all personal data, defined as follows:

- **Confidentiality** means that only people who have a need to know and are authorised to use the personal data can access it.
- **Integrity** means that personal data is accurate and suitable for the purpose for which it is processed.
- **Availability** means that only authorised users can access the personal data when they need it for authorised purposes.

#### 5.9 The Data Protection Officer shall have the following responsibilities:

- Review of all data processing activities (inventory / mapping);
- Conduct of regular health checks/audits and issue recommendations;
- Assist with data protection impact assessments and monitoring performance;
- Monitoring and advice relating to subject access requests and data breaches;
- Assist the organisation with maintenance of records;
- Monitoring and advice relating to FOI and other information requests;
- Co-operation with, and acting as the contact point for the Information Commissioner's Office, who are the supervisory authority in respect of all data protection matters;
- Act as the contact point for data subjects to deal with requests and complaints;
- Training of organisation staff and workforce.

## 6. Data Protection Principles

6.1 Anyone processing personal data must comply with the data protection principles. The organisation will comply and is committed to these principles in relation to any processing of personal data. The Data Protection principals provide that personal data must be:

- **Processed lawfully, fairly and in a transparent manner** in relation to the data subject and their rights;
- **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**

- **Must NOT be transferred to people or organisations situated in other countries without adequate protection.**

## **7. Data Subject's Rights**

7.1 The organisation supports the rights of data subjects (or the parents/carers of data subjects where data subjects are not able to demonstrate the capacity to understand their rights) in relation to data that is processed or stored about them, as follows:

- Right to fair and transparent processing;
- Right of access;
- Right of rectification;
- Right to erasure (the "right to be forgotten");
- The right to restrict processing;
- Right to be notified of erasure, rectification or restriction;
- Right of data portability;
- Right to object to processing;
- Right to object to processing for the purposes of direct marketing;
- Right to object to processing for scientific, historical or statistical purposes;
- Right to not be evaluated on the basis of automated processing;
- Right to withdraw consent at any time;
- Right to be notified about a data breach;
- Right to an effective judicial remedy against a supervisory authority;
- Right to lodge a complaint with supervisory authority;
- Right to an effective judicial remedy against a controller or processor;
- Right to compensation.

7.2 The organisation shall maintain procedures, policies and notices to ensure that data subjects are informed about their rights

## **8. Fair and Transparent Processing of Data**

8.1. Data Protection Legislation is not intended to prevent the processing of personal data, but to ensure that it is done fairly and without adversely affecting the rights of the data subject.

8.2. For personal data to be processed fairly, data subjects must and will be made aware of the following in our privacy notices or requests to process data:

- That the personal data is being processed;
- Why the personal data is being processed;
- What the lawful basis is for that processing (see below);

- Whether the personal data will be shared, and if so with whom;
- The period for which the personal data will be held;
- The right of the data subject to raise a complaint with the Information Commissioner's Office in relation to any processing.

8.3. The organisation will only process data that is **necessary and relevant to the purpose for which it was gathered, and will ensure that we have a lawful basis for any processing.**

8.4 When regulations require it, data collected for the purposes of public health (including visitor contact data for COVID-19) will be kept as long as required. Contact data for visitors will be kept for 21 days after the most recent visit, with information on visitors kept as per standard retention requirements. Public Health data may be shared with third-parties as required including, but not limited to:

- National Health Service (including NHS Test and Trace)
- Public Health England
- Other local health authorities

Data collected and processed for public health purposes is done so under GDPR Article 9(2)(i) which states: (in part) "processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health..." and Recital 54 which includes: "The processing of special categories of personal data may be necessary for reasons of public interest in the areas of public health without consent of the data subject."

8.5 Collection and processing of visitor data will be documented in the privacy notices and in a statement available to visitors at the time of data collection to include the following information:

"We collect the following visitor information for the purposes of security, safety and public health:

- Name
- Organisation
- Date and time of visit
- Car registration
- Contact details

These are kept for six years in case of any claims by students, staff or visitors under the Limitations Act (1980).

Should public health authorities require visitor test and trace logs to be kept (e.g. for COVID-19), relevant visitor data may be shared with such authority. Ensure you sign and display an enhanced privacy notice stating this in any such circumstances and conduct any required risk assessment for visitors.



## 9. Lawful Processing of Data

9.1 For personal data to be processed lawfully it must be processed on the basis on one of the legal grounds set out in the DATA Protection Legislation. The organisation will only process personal data where a lawful basis for processing exists. Specifically, where:

- The data subject 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 (e.g the Education Act 2011);
- Processing is necessary in order to protect the **vital interests** of the data subject or of another natural person;
- Processing is necessary for the **performance of a task carried out in the public interest** or in the exercise of official authority vested in the controller.

## 10. Special Category Data

10.1 This is data relating to **health; race; sexuality; religion; criminal offences; political opinions and union memberships.**

10.2 These special categories of personal data relating to will not be processed unless a specific lawful basis as listed in Article 9 of the GDPR applies. When this special category data is being processed we will normally only do so under the following legal grounds:

- Where the processing is **necessary for employment law** purposes, for example in relation to sickness absence;
- Where the processing is necessary for reasons of substantial public interest, for example for the purposes of equality of opportunity and treatment;
- Where the processing is necessary for **health or social care purposes**, for example in relation to pupils with medical conditions or disabilities; and
- **Where none of the above apply then we will seek the consent of the data subject to the processing of their special category personal data.**

## 11. Consent

11.1 There are strict legal requirements in relation to the form of consent that must be obtained from data subjects.

- 11.2 When pupils join the Organisation a consent form will be required to be completed in relation to them. This consent form deals with:
- display in access-controlled areas of the school (such as corridors, classrooms)
  - display in public areas of the school (such as the reception area)
  - use in the school newsletter and other printed documents we produce for promotional purposes (such as the school prospectus)
  - use on the school website
  - use on social media (such as the school Twitter or Facebook page)
  - School photographs can be provided to the media for publication or broadcast
  - In Early Years, photographs on Tapestry for their learning journals.
- 11.3 Where appropriate third parties may also be required to complete a consent form.
- 11.4 In relation to all pupils under the age of 12 years old we will seek consent from an individual with parental responsibility for that pupil.
- 11.5 We will generally only seek consent directly from a pupil if they are legally able to give such consent. The legal age for consent under Data Protection legislation is 12. However we recognise that this may not be appropriate in certain circumstances and therefore the organisation may be required to seek consent from an individual with parental responsibility.
- 11.6 If consent is required for the processing of personal data of any data subject then the form of this consent must:
- Inform the data subject of exactly what we intend to do with their personal data;
  - Require them to positively confirm that they consent (we cannot ask them to opt-out rather than opt-in); and
  - Inform the data subject of how they can withdraw their consent.
- 11.7 Any **consent must be freely given**, which means that we cannot make the provision of any goods or services or other matter conditional on a data subject giving their consent.
- 11.8 The DPO must always be consulted in relation to any consent form before consent is obtained.
- 11.9 A record must always be kept of any consent, including how it was obtained and when.
- 11.10 There may be circumstances where it is considered necessary to process personal data or special category personal data in order to protect the vital interests of a data subject. This might include safeguarding, child protection and medical emergencies where the data subject is not in a position to give

consent to the processing. We believe that this will only occur in very specific and limited circumstances. In such circumstances we would usually seek to consult with the DPO in advance, although there may be emergency situations where this does not occur. Please refer to the organisation Safeguarding Policy, Child Protection Policy and organisation Medical Policy for further information.

## **12. Disclosure and Sharing of Personal Information**

- 12.1 We may share personal data that we hold about data subjects, with other organisations, without consent, where we have a lawful basis for doing so. Such organisations include the Department for Education and Education and Skills Funding Agency "ESFA", Ofsted, health authorities and professionals, the Local Authority, examination bodies, other organisations, and other organisations where we have a lawful basis for doing so.
- 12.2 The organisation will inform data subjects of any sharing of their personal data unless we are not legally required to do so, for example where personal data is shared with the police in the investigation of a criminal offence.
- 12.3 In some circumstances we will not share safeguarding information. Please refer to our Child Protection Policy.
- 12.4 Further detail is provided in our Schedule of Processing Activities.

## **13. Data Security**

- 13.1 The organisation will implement appropriate data security measures using policies, procedures and technologies that ensure and maintain the security of all personal data from the point of collection to the point of destruction.
- 13.2 These security measures will be appropriate to the risks in processing personal data and will be consistent with the rights of the data subjects.
- 13.3 These measures shall include as appropriate:
  - Measures and data access controls to ensure that the Personal Data can only be accessed by authorised personnel for the purposes agreed in the record of processing activity and outlined in the organisation privacy notice;
  - In assessing the appropriate level of security, account shall be taken in particular of all the risks that are presented by processing, for example from accidental or unlawful destruction, loss, or alteration, unauthorised or unlawful storage, processing, access or disclosure of personal data;
  - The anonymisation, pseudonymisation and encryption of personal data;

- The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
- Measures to identify vulnerabilities with respect to the processing of personal data in systems used to provide services to The Organisation.
- Adherence to an Acceptable Use Policy when using technology to ensure the security and confidentiality of personal data when using all systems (including email) in all environments across the organisation.
- Any email, messages or notifications should never be read in the vicinity of children, or other unauthorised individuals
- Email classification should be in place, and emails flagged (or described in the subject line) as "Sensitive/Highly Sensitive" when appropriate

## **14. Data Protection Impact Assessments**

- 14.1 The organisation takes data protection very seriously, and will consider and comply with the requirements of Data Protection Legislation in relation to all of its activities whenever these involve the use of personal data, in accordance with the principles of data protection by design and default.
- 14.2 In certain circumstances the law requires us to carry out detailed assessments of proposed processing. This includes where we intend to use new technologies which might pose a high risk to the rights of data subjects because of the types of data we will be processing or the way that we intend to do so.
- 14.3 The organisation will complete an assessment of any such proposed processing and will use a template document which ensures that all relevant matters are considered.
- 14.4 The DPO should always be consulted as to whether a data protection impact assessment is required, and if so how to undertake that assessment.

## **15. Data Breaches**

- 15.1 All stakeholders are responsible for reporting known breaches internally to a senior manager or to the Data Protection Officer as soon as the breach is recognised. The responsible member of the senior leadership team should be informed.
- 15.2 The organisation will keep and implement a dedicated Data Breach Procedure to ensure any personal data breaches, including the facts relating

to the data breach, its effects and the remedial action taken, are recorded in a data breach log and acted on accordingly.

- 15.3 The log shall be monitored and assessed by the Data Protection Officer. It will enable them to verify compliance with the data breach rules and raise awareness of minor breaches that may assist in identifying new data handling processes and training requirements
- 15.4 In the case of a personal data breach resulting in a likely risk to the rights and freedoms of natural persons, and after consultation with the Data Protection Officer, the organisation 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.
- 15.5 Where the notification to the Information Commissioner's Office is not made within 72 hours, it shall be accompanied by reasons for the delay.
- 15.6 In order to evaluate the personal data breach, the organisation shall, without undue delay, immediately 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.
- 15.7 **The notification to the Information Commissioner's Office 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 points 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.
- 15.8 Where breaches are reportable to the Information Commissioner's Office, the senior leadership team should immediately inform members of the organisation's appropriate governance board or risk committee.
- 15.9 For examples of data breaches, please see Appendix 2

## **16. Subject Access Requests**

- 16.1 The organisation 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.

- 16.2 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.

- 16.3 **For information and guidance on how the organisation will deal with a Subject Access Request see the Subject Access Request Procedure.**

## 17. Publication of Information

- 17.1 The organisation maintains and publishes a publication scheme on its website outlining classes of information that will be made routinely available, including policies and procedures.
- 17.2 Classes of information specified in the publication scheme will be made available quickly and easily on request.
- 17.3 The organisation will not publish any personal information, including photos, on its website without the permission of the affected individual.
- 17.4 When uploading information to the organisation website, staff will be considerate of any metadata or deletions which could be accessed in documents and images on the site.

## 18. DBS Data

- 18.1 All data provided by the DBS will be handled in line with data protection legislation; this includes electronic communication.

- 18.2 Data provided by the DBS will never be duplicated.
- 18.3 Any third parties who access DBS information will be made aware of the data protection legislation, as well as their responsibilities as a data handler.
- 18.4 Data Subjects have the right to appeal against any automated decision making, such as a DBS check.

## **19. Photography Images and Videos**

- 19.1 Photographs and videos will only be collected and stored by the organisation, organisation staff and workforce with a documented lawful basis as in accordance with the organisation Photography Images and video policy document.
- 19.2 Photographs and videos will normally only be taken and used where they are deemed essential for performing the public task of the organisation or relative to providing education.
- 19.3 However there may be occasions that arise where the organisation would like to celebrate the achievements of our pupils and therefore we may want to use images and videos of our pupils within promotional materials, or for publication in the media such as local, or even national, newspapers covering organisation events or achievements. If this is the case we will seek the consent of the pupils, and their parents where appropriate, before allowing the use of images or videos of pupils for such purposes.
- 19.4 Where photographs are required for other purposes, these purposes will be documented and explicit consent will be sought.
- 19.5 The retention period for photographs and videos taken by the organisation, organisation staff and workforce will be documented in the organisation retention policy. At the end of the retention period photographs will either be destroyed or they may be retained as photos for archiving purposes in the public interest.
- 19.6 Parents and others attending organisation events are allowed to take photographs and videos of those events for domestic purposes. For example, parents can take video recordings of an organisation performance involving their child. The organisation does not prohibit this as a matter of policy.
- 19.7 The organisation does not however agree to any such photographs or videos being used for any other purpose, but acknowledges that such matters are, for the most part, outside of the ability of the organisation to control or prevent.
- 19.8 The organisation asks that parents and others do not post any images or



videos which include any child other than their own child on any social media or otherwise publish those images or videos.

- 19.9 Whenever a pupil begins their attendance at the organisation they, or their parent where appropriate, will be asked to complete a consent form in relation to the use of images and videos of that pupil. We will not use images or videos of pupils for any purpose where we do not have consent.

## **21. Retention Policy**

- 21.1 The organisation will not keep personal data longer than necessary and will maintain a retention schedule outlining the retention requirements of electronic and paper records. The Organisation will retain the minimum amount of information that it requires to carry out its' statutory functions and the provision of services.
- 21.2 In circumstances where a retention period of a specific document has expired, checks will be made to confirm disposal and consideration given to the method of disposal to be used based on the data to be disposed of.
- 21.3 These checks will include the following questions being addressed:
- Have the documents been checked to ensure they are appropriate for destruction?
  - Is retention required to fulfil statutory obligations or other regulatory obligations, including child protection?
  - Is retention required for evidence?
  - Is retention required to meet the operational needs of the service?
  - Is retention required because the document or record is of historic interest, intrinsic value or required for organisational memory?
- 21.4 For SCPS Annual Data Retention Checklist see Appendix 4
- 21.5 Staff and Governors will be requested to complete a declaration annually to confirm that to the best of their knowledge they have completed an audit of their working environments and personal drives, ensuring data held is disposed in line with the retention policy timescales. The Head Teacher will sign the annual audit on the basis staff have signed these declarations.

## **22. Training**

- 22.1 The organisation shall ensure that all members of staff receive data protection training, including training on information handling appropriate to ensure data protection competence in their role. This training shall be completed every two years as a minimum.



## **23. Data Processors**

- 23.1 The organisation contract with various organisations who provide services to the organisation, including:
- Payroll Providers – to enable us to pay our employees;
  - Parent payment systems – to enable parents to pay for organisation meals, trips and/or uniforms;
  - Pupil Assessment systems – to support us with the tracking and monitoring of pupil achievement;
  - Communication systems – to enable us to effectively communicate with parent and pupils;
  - organisation meal providers – to support with the provision and payment for organisation meals;
  - Photographers – to enable us to store pupil photographs for safeguarding purposes;
  - HR Systems – for the effective management of all aspects of staff management;
- 23.2 In order that these services can be provided effectively we are required to transfer personal data of data subjects to these data processors.
- 23.3 Personal data will only be transferred to a data processor if they agree to comply with our procedures and policies in relation to data security, or if they put in place adequate measures themselves to the satisfaction of the organisation.
- 23.4 The organisation will always undertake due diligence of any data processor before transferring the personal data of data subjects to them.
- 23.5 Contracts with data processors will comply with Data Protection Legislation and contain explicit obligations on the data processor to ensure compliance with the Data Protection Legislation, and compliance with the rights of Data Subjects.

## **24. Changes to this Policy**

- 24.1 We may change this policy at any time. Where appropriate, we will notify data subjects of those changes.

## Appendix 1: GDPR Definitions

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

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

**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 organisational 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;

**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; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;

**Processor** means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;

**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 with Union or Member State 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

**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 a Member State pursuant to Article 51 of the GDPR;

**Cross-border processing** means either:

- processing of personal data which takes place in the context of the activities of establishments in more than one Member State of a controller or processor in the Union where the controller or processor is established in more than one Member State; or
- processing of personal data which takes place in the context of the activities of a single establishment of a controller or processor in the Union but which substantially affects or is likely to substantially affect data subjects in more than one Member State;
- **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 organisation** means an organisation 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 or data concerning a natural person's sex life or sexual orientation;
- **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 2: 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 Organisation, 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.

### Examples of Breaches caused by IT Security Incidents:

- 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.

### Appendix 3: Dealing with Subject Access Requests

What must the school do?	Why?	How?
We must be clear about the nature of the request and identify what information is being requested.	Being clear about the nature of the request will enable you to decide whether the request needs to be dealt with in accordance with statutory requirements, who needs to deal with the request, and/or whether this is business as usual (BAU). If needed ask the submitter of the request for clarity.	<p>Review the request and identify:</p> <p>If the request is for the personal information of the requester or made by an individual on behalf of another person (e.g. on behalf of a child or an adult lacking capacity) – this is a subject access request;</p> <p>If the request is for non-personal information – this may be dealt with as BAU or formally under the Freedom of Information Act 2000 (the FOIA) or the Environmental Information Regulations 2004 (the EIR).</p> <p>NB: The request can be received in a range of different formats e.g. letter, email, a completed form, or can be made via social media (e.g. a Facebook page or Twitter account).</p>
If the request is a SAR the request must be forwarded to the responsible member of staff (usually the Headteacher) and the Data Protection Officer within two working days of receipt of the request.	The GDPR stipulates that SARs must be completed within one month of the request – but in reality, as soon as possible.	Log the SAR in the subject access request log and inform all appropriate staff required to deal with the request.

<p>If the information requested is for non-personal information i.e. is organisational or statistical information, this will fall under the FOIA or EIR, or BAU and will be dealt with, as follows:</p> <p>All non-routine FOIA or EIR requests must be forwarded to the responsible member of staff (usually the Headteacher) and the Data Protection Officer within two working days of receipt of the request.</p>	<p>The FOIA and EIR stipulates that requests must be completed within 20 working days of the request – therefore the more swiftly request are being dealt with, the more likely The Organisation will meet its statutory deadlines.</p> <p>BAU requests need to be dealt with by an individual in that particular service area who can identify and locate the information requested and provide a response within a reasonable timeframe.</p>	<p>If the request is for non-routine/FOIA/EIR information contact the responsible member of staff (usually the Headteacher) and the Data Protection Officer.</p>
<p>If the information requested is for the personal information of an individual for use in a criminal investigation by the police, or any other agency investigating criminal offences, this will fall under either the regulatory Investigative Powers Act 2000 (RIPA) or Data Protection Act 2018.</p> <p>The request can be for either hard copy or any type of electronic information including email traffic ie the time and information that an email is sent.</p> <p>The request must be forwarded to the responsible member of staff (usually the Headteacher) and the Data Protection Officer within two days.</p>	<p>It is in the public interest that requests are identified and dealt with as quickly as possible.</p>	<p>Scan and email the request to the responsible member of staff (usually the Headteacher) and the Data Protection Officer as needed.</p>

## Appendix 4: Annual review of school records and safe data destruction checklist.

### Completion page

School name: Sheringham Community Primary School and Nursery

Review completed by: \_\_\_\_\_

Date: \_\_\_\_\_

Approved by Headteacher: \_\_\_\_\_

Date: \_\_\_\_\_

*Note – The completion of this review should be shared at the Governors meeting and minuted.*

### A. Summary of areas reviewed:

Ref	Area	Pages	Annual Review	Reviewer Initials
1	Management of the School	5 to 9		
2	Human Resources	10 to 12		
3	Financial Management of the School	13 to 14		
4	Property Management	15		
5	Pupil Management	16 to 17		
6	Curriculum Management	18		
7	Extra-Curricular Activities	19 to 20		
8	Central Government and Local Authority	21		
9	List of School Records and Data safely	22		



## Contents

- A. Aims 25
  - B. Safe Destruction of Data
    - (i) Disposal of records that have reached the end of the minimum retention period allocated
    - (ii) Safe destruction of records
    - (iii) Freedom of Information Act 2000 (FoIA 2000)
  - 1. Management of the School
  - 2. Human Resources
  - 3. Financial Management of the School
  - 4. Property Management
  - 5. Pupil Management
  - 6. Curriculum Management
  - 7. Extra Curriculum Management
  - 8. Central Government and Local Authority
- Appendix A – List of School Records and Data safely destroyed

---

### 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 Managers, Clerks, SENCO 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.

If you have any queries in completing this checklist please contact:

The Data Protection Officer  
Data Protection Education  
1 Saltmore Farm  
New Inn Road  
Hinxworth  
Baldock  
SG7 5EZ

Email: [info@dataprotectioneducation.com](mailto:info@dataprotectioneducation.com)  
Phone: 0800 0862018

---

### Version Control History

First Edition – June 2018

## 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 <sup>1</sup>	
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 <sup>2</sup>		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	

<sup>1</sup> 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.

<sup>2</sup> 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.

<b>1.1 Governing Body (continued...)</b>					
<b>Ref</b>	<b>Basic file description</b>	<b>Data Protection Issues</b>	<b>Retention Period [Operational]</b>	<b>Action at the end of the administrative life of the record</b>	<b>Annual Review Completed Tick (✓)</b>
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	
1.1.5	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	

<b>1.1 Governing Body (continued...)</b>					
<b>Ref</b>	<b>Basic file description</b>	<b>Data Protection Issues</b>	<b>Retention Period [Operational]</b>	<b>Action at the end of the administrative life of the record</b>	<b>Annual Review Completed Tick (✓)</b>
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	

<b>1.2 Head Teacher and Senior Management Team</b>					
<b>Ref</b>	<b>Basic file description</b>	<b>Data Protection Issues</b>	<b>Retention Period [Operational]</b>	<b>Action at the end of the administrative life of the record</b>	<b>Annual Review Completed Tick (✓)</b>
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	

<b>1.2 Head Teacher and Senior Management Team (continued...)</b>					
<b>Ref</b>	<b>Basic file description</b>	<b>Data Protection Issues</b>	<b>Retention Period [Operational]</b>	<b>Action at the end of the administrative life of the record</b>	<b>Annual Review Completed Tick (✓)</b>
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	



<b>1.3 Admissions Process</b>					
<b>Ref</b>	<b>Basic file description</b>	<b>Data Protection Issues</b>	<b>Retention Period [Operational]</b>	<b>Action at the end of the administrative life of the record</b>	<b>Annual Review Completed Tick (✓)</b>
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. <sup>3</sup>	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	

<b>1.3 Admissions Process (continued...)</b>					
<b>Ref</b>	<b>Basic file description</b>	<b>Data Protection Issues</b>	<b>Retention Period [Operational]</b>	<b>Action at the end of the administrative life of the record</b>	<b>Annual Review Completed Tick (✓)</b>
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	

<b>1.4 Operational Administration</b>					
<b>Ref</b>	<b>Basic file description</b>	<b>Data Protection Issues</b>	<b>Retention Period [Operational]</b>	<b>Action at the end of the administrative life of the record</b>	<b>Annual Review Completed Tick (✓)</b>
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 Electronic Sign In System 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.*

<b>2.1 Recruitment</b>					
<b>Ref</b>	<b>Basic file description</b>	<b>Data Protection Issues</b>	<b>Retention Period [Operational]</b>	<b>Action at the end of the administrative life of the record</b>	<b>Annual Review Completed Tick (✓)</b>
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	
2.1.3	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		

<b>2.1 Recruitment (continued...)</b>					
<b>Ref</b>	<b>Basic file description</b>	<b>Data Protection Issues</b>	<b>Retention Period [Operational]</b>	<b>Action at the end of the administrative life of the record</b>	<b>Annual Review Completed Tick (✓)</b>
2.1.6	Pre-employment vetting information – Evidence proving the right to work in the United Kingdom <sup>4</sup>	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		

<b>2.2 Operational Staff Management</b>					
<b>Ref</b>	<b>Basic file description</b>	<b>Data Protection Issues</b>	<b>Retention Period [Operational]</b>	<b>Action at the end of the administrative life of the record</b>	<b>Annual Review Completed Tick (✓)</b>
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	

<b>2.3 Management of Disciplinary and Grievance Processes</b>					
<b>Ref</b>	<b>Basic file description</b>	<b>Data Protection Issues</b>	<b>Retention Period [Operational]</b>	<b>Action at the end of the administrative life of the record</b>	<b>Annual Review Completed Tick (✓)</b>
2.3.1	Allegation of a child protection nature against a member of staff including where the allegation is unfounded <sup>5</sup>	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	

<b>2.4 Health and Safety</b>					
<b>Ref</b>	<b>Basic file description</b>	<b>Data Protection Issues</b>	<b>Retention Period [Operational]</b>	<b>Action at the end of the administrative life of the record</b>	<b>Annual Review Completed Tick (✓)</b>
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	

<b>2.4 Payroll and Pensions</b>					
<b>Ref</b>	<b>Basic file description</b>	<b>Data Protection Issues</b>	<b>Retention Period [Operational]</b>	<b>Action at the end of the administrative life of the record</b>	<b>Annual Review Completed Tick (✓)</b>
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*

<b>3.1 Risk Management and Insurance</b>					
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	

<b>3.2 Asset Management</b>					
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	

<b>3.3 Accounts and Statements including Budget Management</b>					
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	

<b>3.4 Contract Management</b>					
<b>Ref</b>	<b>Basic file description</b>	<b>Data Protection Issues</b>	<b>Retention Period [Operational]</b>	<b>Action at the end of the administrative life of the record</b>	<b>Annual Review Completed Tick (✓)</b>
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	

<b>3.5 School Fund</b>					
<b>Ref</b>	<b>Basic file description</b>	<b>Data Protection Issues</b>	<b>Retention Period [Operational]</b>	<b>Action at the end of the administrative life of the record</b>	<b>Annual Review Completed Tick (✓)</b>
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	

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	

<b>3.6 School Meals</b>					
<b>Ref</b>	<b>Basic file description</b>	<b>Data Protection Issues</b>	<b>Retention Period [Operational]</b>	<b>Action at the end of the administrative life of the record</b>	<b>Annual Review Completed Tick (✓)</b>
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.*

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

<b>4.2 Maintenance</b>					
<b>Ref</b>	<b>Basic file description</b>	<b>Data Protection Issues</b>	<b>Retention Period [Operational]</b>	<b>Action at the end of the administrative life of the record</b>	<b>Annual Review Completed Tick (✓)</b>
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*

<b>5.1 Pupil's Educational Record</b>					
<b>Ref</b>	<b>Basic file description</b>	<b>Data Protection Issues</b>	<b>Retention Period [Operational]</b>	<b>Action at the end of the administrative life of the record</b>	<b>Annual Review Completed Tick (✓)</b>
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. <sup>3</sup>	
	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		

<sup>3</sup> 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

<b>5.1 Pupil's Educational Record (continued...)</b>					
<b>Ref</b>	<b>Basic file description</b>	<b>Data Protection Issues</b>	<b>Retention Period [Operational]</b>	<b>Action at the end of the administrative life of the record</b>	<b>Annual Review Completed Tick (✓)</b>
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	

<b>5.2 Attendance</b>					
<b>Ref</b>	<b>Basic file description</b>	<b>Data Protection Issues</b>	<b>Retention Period [Operational]</b>	<b>Action at the end of the administrative life of the record</b>	<b>Annual Review Completed Tick (✓)</b>
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	

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



<b>5.3 Special Educational Needs (continued...)</b>					
<b>Ref</b>	<b>Basic file description</b>	<b>Data Protection Issues</b>	<b>Retention Period [Operational]</b>	<b>Action at the end of the administrative life of the record</b>	<b>Annual Review Completed Tick (✓)</b>
			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		<p>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.</p> <p>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</p>	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	

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

<b>7.1 Educational Visits outside the Classroom</b>					
<b>Ref</b>	<b>Basic file description</b>	<b>Data Protection Issues</b>	<b>Retention Period [Operational]</b>	<b>Action at the end of the administrative life of the record</b>	<b>Annual Review Completed Tick (✓)</b>
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		

<b>7.2 Walking Bus</b>					
<b>Ref</b>	<b>Basic file description</b>	<b>Data Protection Issues</b>	<b>Retention Period [Operational]</b>	<b>Action at the end of the administrative life of the record</b>	<b>Annual Review Completed Tick (✓)</b>
7.2.1	Walking Bus Registers	Yes	<p>Date of register + 3 years</p> <p>This takes into account the fact that if there is an incident requiring an accident report the register will be submitted with the accident report and kept for the period of time required for accident reporting</p>	<p>SECURE DISPOSAL</p> <p>[If these records are retained electronically any back up copies should be destroyed at the same time]</p>	

<b>7.3</b>					
<b>Ref</b>	<b>Basic file description</b>	<b>Data Protection Issues</b>	<b>Retention Period [Operational]</b>	<b>Action at the end of the administrative life of the record</b>	<b>Annual Review Completed Tick (✓)</b>
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

<b>8.1 Local Authority</b>					
<b>Ref</b>	<b>Basic file description</b>	<b>Data Protection Issues</b>	<b>Retention Period [Operational]</b>	<b>Action at the end of the administrative life of the record</b>	<b>Annual Review Completed Tick (✓)</b>
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	

<b>8.2 Central Government</b>					
<b>Ref</b>	<b>Basic file description</b>	<b>Data Protection Issues</b>	<b>Retention Period [Operational]</b>	<b>Action at the end of the administrative life of the record</b>	<b>Annual Review Completed Tick (✓)</b>
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 A – List of School Records and Data safely destroyed  
The following sheet can be completed or alternatively documented in a spreadsheet.

File/Record Title	Description	Reference or Cataloguing Information	Number of Files Destroyed	Method of destruction	<u>Confirm</u> (i) Safely destroyed (ii) In accordance with Data Retention Guidelines Tick (v)	<u>Added to spreadsheet</u> Yes/No
School Invoices	Copies of purchase invoices dated 2011/12	Folders marked "Purchase Invoices 2011/12" 1 to 3	3 Folders	Shredding	v	