HUNDON AND THURLOW PRIMARY FEDERATION

Laying the foundations for a bright future

The Parable of The Wise and The Foolish Man

(Matthew, Chapter 7, verses 24 to 27 and the Gospel of Luke, Chapter 6, verses 46 to 49)

Data Protection Policy

NB: This policy has been discussed and considered for equality giving consideration to the protected characteristics- gender, age, race, disability, religion or belief, sexual orientation, gender reassignment, pregnancy or maternity and any other recognised area of discrimination.

Approved by:	Chair Of Governors	**Date:** Autumn 2022
Last reviewed on:	Autumn 2022	
Next review due by:	Autumn 2024	

Contents

1. Aims

Our school aims to ensure that all personal data collected about staff, pupils, parents, governors, visitors and other individuals is collected, stored and processed in accordance with the General Data Protection Regulation (EU) 2016/679 (GDPR) and the Data Protection Act 2018 (DPA 2018).

This policy applies to all personal data, regardless of whether it is in paper or electronic format.

2. Legislation and guidance

This policy meets the requirements of the GDPR and the provisions of the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the GDPR.

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.

3. Definitions

Term	Definition
Personal data	Any information relating to an identified, or identifiable, living individual. This may include the individual's: • Name (including initials) • Identification number • Location data • Online identifier, such as a username It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.
Special categories of personal data	Personal data which is more sensitive and so needs more protection, including information about an individual's: • Racial or ethnic origin • Political opinions • Religious or philosophical beliefs • Trade union membership • Genetics • Health – physical or mental • Sex life or sexual orientation
Processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.
Data subject	The identified or identifiable individual whose personal data is held or processed.
Data controller	A person or organisation that determines the purposes and the means of processing of personal data.
Data processor	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

4. The data controller

Our school processes personal data relating to parents, pupils, staff, governors, visitors and others, and therefore is a data controller.

The school is registered as a data controller with the ICO and has paid its data protection fee to the ICO, as legally required.

5. Roles and responsibilities

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

5.1 Governing board

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

5.2 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.

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

Full details of the DPO's responsibilities are set out in their job description.

Our DPO is Sara Clark and is contactable via email at saraclarkdpo@hundonschool.co.uk

5.3 Headteacher

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

5.4 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 European Economic Area
    - If there has been a data breach
    - Whenever they are engaging in a new activity that may affect the privacy rights of individuals
    - If they need help with any contracts or sharing personal data with third parties

6. Data protection principles

The GDPR is based on data protection principles that our school must comply with.

The principles say that personal data must be:

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes

- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed
- Accurate and, where necessary, kept up to date
- Kept for no longer than is necessary for the purposes for which it is processed
- Processed in a way that ensures it is appropriately secure

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

7. Collecting personal data

7.1 Lawfulness, fairness and 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 needs to be processed so that the school can **fulfil a contract** with the individual, or the individual has asked the school to take specific steps before entering into a contract
- The data needs to be processed so that the school can **comply with a legal obligation**
- The data needs to be processed to ensure the **vital interests** of the individual or another person i.e. to protect someone's life
- The data needs to be processed so that the school, as a public authority, can **perform a task in the public interest or exercise its official authority**
- The data needs to be processed for the **legitimate interests** of the school (where the processing is not for any tasks the school performs as a public authority) or a third party, provided the individual's rights and freedoms are not overridden
- The individual (or their parent/carer when appropriate in the case of a pupil) has freely given clear **consent**

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.

If we offer online services to pupils, such as classroom apps, and we intend to rely on consent as a basis for processing, we will get parental consent (except for online counselling and preventive services).

7.2 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 which can be found as an appendix to this policy **- Appendix 3**.

8. Sharing personal data

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 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.

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

9. Subject access requests and other rights of individuals

9.1 Subject access requests

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 they must immediately forward it to the DPO. A template form is included in this policy as **Appendix 1.**

9.2 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.

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.

9.3 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.

9.4 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 (see section 7), 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.

10. 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.

11. Photographs and videos

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

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

Any photographs and videos taken by parents/carers at school events for their own personal use are not covered by data protection legislation. However, 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.

Where photographs and names are used by the media, we have specifically requested consent from our parents for this and will only use first names to accompany them.

See our safeguarding policy for more information on our use of photographs and videos.

12. 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 privacy 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 European Economic Area (EEA), where different data protection laws will 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 EEA and the safeguards for those, retention periods and how we are keeping the data secure

13. 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 Information Management 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)

14. 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.

15. Personal data breaches

The school will make all reasonable endeavours to ensure that there are no personal data breaches.

In the unlikely event of a suspected data breach, we will follow the procedure set out in **appendix 2**.

When appropriate, we will report the data breach to the ICO within 72 hours after becoming aware of it. Such breaches in a school context may include, but are not limited to:

- A non-anonymised dataset being published on the school website which shows the exam results of pupils eligible for the pupil premium
- Safeguarding information being made available to an unauthorised person
- The theft of a school laptop containing non-encrypted personal data about pupils

16. 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.

17. Monitoring arrangements

The DPO is responsible for monitoring and reviewing this policy.

This policy will be reviewed **every 2 years** and shared with the full governing board.

18. Links with other policies

This data protection policy is linked to our:

- Freedom of information publication scheme
- Information Management Policy
- Safeguarding Policy

19. Appendices

- Appendix 1. Subject Access Request Form
- Appendix 2. Personal Data Breach Procedure
- Appendix 3. Data Retention Schedule

Appendix 1: Subject Access Request Form

Date:

Hundon and Thurlow Primary Federation

Re: subject access request

Dear *Sara Clark*

Please provide me with the information about me that I am entitled to under the General Data Protection Regulation. This is so I can be aware of the information you are processing about me, and verify the lawfulness of the processing.

Here is the necessary information:

Name	
Relationship with the school	Please select: Pupil / parent / employee / governor / volunteer Other (please specify):
Correspondence address	
Contact number	
Email address	
Details of the information requested	Please provide me with: *Insert details of the information you want that will help us to locate the specific information. Please be as precise as possible, for example:* • *Your personnel file* • *Your child's medical records* • *Your child's behavior record, held by [insert class teacher]* • *Emails between 'A' and 'B' between [date]*

If you need any more information from me, please let me know as soon as possible.

Please bear in mind that under the GDPR you cannot charge a free to provide this information, and in most cases, must supply me with the information within 1 month.

If you need any advice on dealing with this request, you can contact the Information Commissioner's Office on 0303 123 1113 or at www.ico.org.uk

Yours sincerely,

Appendix 2: Personal data breach procedure

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

- On finding or causing a breach, or potential breach, the staff member, governor or data processor must immediately notify the DPO by email saraclarkdpo@hundonschool.co.uk
- The DPO 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
- The DPO will alert the headteacher and the chair of governors
- The DPO will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary. (Actions relevant to specific data types are set out 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
- The DPO will work out whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the DPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:
    - Loss of control over their data
    - Discrimination
    - Identify theft or fraud
    - Financial loss
    - Unauthorised reversal of pseudonymisation (for example, key-coding)
    - Damage to reputation
    - Loss of confidentiality
    - Any other significant economic or social disadvantage to the individual(s) concerned

  If it's likely that there will be a risk to people's rights and freedoms, the DPO must notify the ICO.
- The DPO will document the decision (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored on the school's computer system.
- Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website, or through their breach report line (0303 123 1113), within 72 hours. 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. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible
- The DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPO will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:
    - The name and contact details of the DPO
    - A description, in clear and plain language, of the nature of the personal data breach
    - 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

As above, any decision on whether to contact individuals will be documented by the DPO.

- The DPO will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies
- The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:
    - Facts and cause
    - Effects
    - Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)

  Records of all breaches will be stored on the school's computer system.
- The DPO and headteacher will meet regularly to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible

Actions to minimise the impact of data breaches

We will take the actions set out below to mitigate the impact of different types of data breach, 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.

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 coordinator 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, the DPO will consider whether it is 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 designated safeguarding lead and discuss whether the school should inform any, or all, of its 3 local safeguarding partners.*

Non-anonymised pupil exam results or staff pay information being shared with governors

- *If Non-anonymised pupil exam results or staff pay information is accidentally made available to governors, the information must be re-called as soon as we become aware of the error*
- *Members of the governing body who receive personal data sent in error must alert the sender and the DPO as soon as they become aware of the error*
- *In any cases where the recall of information is unsuccessful, the DPO will contact the relevant unauthorised individuals who received the information, explain that the information was sent in error, and request that those individuals delete/destroy the information and do not share, publish, save or replicate it in any way*
- *The DPO will ensure we receive a written response from all the individuals who received the data, confirming that they have complied with this request*

A school laptop containing non-encrypted sensitive personal data being stolen or hacked

- *Members of staff must alert the sender and the DPO as soon as they become aware of the incident*
- *The DPO will contact the school ICT coordinator for further guidance on how to limit data loss*

Appendix 3: Data Retention Schedule

1 Governing body

For further information about governing body records please see: “The constitution of governing bodies of maintained schools statutory guidance for governing bodies of maintained schools and local authorities in England August 2017”

1.1 Management of Governing Body					
	Basic file description	Personal Information	Statutory provisions	Retention period	Action at end of the administrative life of the record
1.1.1	Instruments of Government			For the life of the school	Consult local archives before disposal
1.1.2	Trusts and endowments			For the life of the school	Consult local archives before disposal
1.1.3	Records relating to the election of parent and staff governors not appointed by the governors	Yes		Date of the election + 6 months	SECURE DISPOSAL
1.1.4	Records relating to the appointment of co-opted governors	Yes		Provided the decision has been recorded in the minutes, these can be destroyed upon the co-opted governors end of office (except in the case of allegations concerning children, then its 25 years)	SECURE DISPOSAL
1.1.5	Records relating to the election of chair or vice chair	Yes		Can be destroyed once the decision is recorded in the minutes	SECURE DISPOSAL
1.1.6	Scheme of delegation and terms of			Until superseded or whilst relevant	These could be offered to local

	reference for committees				archives
1.1.7	Meetings schedule			Current year	STANDARD DISPOSAL
1.1.8	Agendas –principal copy	Potential		Store with the principal set of minutes	Consult local archives before disposal
1.1.9	Minutes – principal copy (signed)	Potential		10 years from the date of the meeting	Consult local archives before disposal
1.1.10	Reports made to governors' meeting which are referred to in the minutes	Potential		10 years from the date of the meeting	Consult local archives before disposal
1.1.11	Registers of attendance at FGB meetings	Yes		Date of the last meeting in the book + 6 years	SECURE DISPOSAL
1.1.12	Papers relating to the management of annual parents meeting	Yes		Date of meeting + 6 years	SECURE DISPOSAL
1.1.13	Agendas – additional copies			Date of meeting	STANDARD DISPOSAL
1.1.14	Records relating to Governor monitoring visits	Yes		Date of the visit + 3 years	SECURE DISPOSAL
1.1.15	Annual reports required by the DoE			Date of the report + 10 years	SECURE DISPOSAL
1.1.16	All records relating to the conversion of schools to Academy status			For the life of the organisation	Consult local archives before disposal

1.1.17	Records relating to complaints made to and investigated by the Governing body or Headteacher	Yes		Major complaints current year + 6 years. Involving negligence then current year + 15 years. Involving child protection or safeguarding issues current year + 40 years	SECURE DISPOSAL
1.1.18	Correspondence sent and received by the Governing body or Headteacher	Potential		General correspondence current year + 3 years	SECURE DISPOSAL
1.1.19	Action plans created and administered by the Governing body	Yes		Until superseded or whilst relevant	SECURE DISPOSAL
1.1.20	Policy documents created and administered by the governing body	Yes		Until superseded	

1.2 Governor Management					
	Basic file description	Personal information	Statutory provisions	Retention period	Action at end of the administrative life of the record
1.2.1	Records relating to the appointment of a clerk to the governing body	Yes		Date appointment ceases + 6 years	SECURE DISPOSAL
1.2.2	Records relating to the terms of office of serving governors, including evidence of Date appointment ceases + 6 years appointment	Yes		Date appointment ceases + 6 years	

1.2.3	Records relating to governor declaration against disqualification criteria	Yes		Date appointment ceases + 6 years	SECURE DISPOSAL
1.2.4	Register of business interests	Yes		Date appointment ceases + 6 years	SECURE DISPOSAL
1.2.5	Governors code of conduct			One copy of each version should be kept for the life of the organisation	
1.2.6	Records relating to the training required and received by Governors	Yes		Date Governor steps down + 6 years	SECURE DISPOSAL
1.2.7	Records relating to the induction programme for new governors	Yes		Date appointment ceases + 6 years	SECURE DISPOSAL
1.2.8	Records relating to DSB checks	Yes		Date of DBS check + 6 years	SECURE DISPOSAL
1.2.9	Governor personnel files	Yes		Date appointment ceases + 6 years	SECURE DISPOSAL

2.1 Headteacher and Senior Management Team					
	Basic file description	Personal information	Statutory provisions	Retention period	Action at end of the administrative life of the record
2.1.1	Log books of activity in the school maintained by the Headteacher	Potential		Date of last entry in the book + 6 years	If of permanent historic value then offer to County Archive Service
2.1.2	Minutes of the Senior Management Team and other internal administrative bodies	Potential		Date of the meeting + 3 years then review annually	SECURE DISPOSAL
2.1.3	Reports created by the Head Teacher or the Management Team	Potential		Date of the report + a minimum of 3 years then review annually	SECURE DISPOSAL
2.1.4	Records created by Head Teacher or other members of staff with administrative responsibilities	Potential		Current academic year + 6 years then review annually	SECURE DISPOSAL
2.1.5	Correspondence created by Head Teacher or other members of staff with administrative responsibilities	Potential		Current year + 3 years	SECURE DISPOSAL
2.1.6	Professional development plans	Potential		These should be held on the individuals personnel record and then held until termination of employment + 6 years	SECURE DISPOSAL

2.1.7	School development plans			Life of the plan + 3 years	SECURE DISPOSAL

2.2 Operational Administration					
	Basic file description	Personal Information	Statutory provisions	Retention period	Action at end of the administrative life of the record
2.2.1	General file series which do not fit under any other category	Potential		Current year + 5 years, then review	SECURE DISPOSAL
2.2.2	Records relating to the creation and publication of the school brochure or prospectus			Current academic year + 3 years	STANDARD DISPOSAL
2.2.3	Records relating to the creation and distribution of circulars to staff, parents or pupils			Current academic year + 1 year	STANDARD DISPOSAL
2.2.4	School Privacy Notice			Until superseded + 6 years	
2.2.5	Consents relating to school activities as part of GDPR compliance	Yes		Whilst the pupil is at the school, then destroy	SECURE DISPOSAL
2.2.6	Newsletters and other items with short operational use			Current academic year + 1 year	STANDARD DISPOSAL

2.2.7	Visitor management systems (signing in sheets)	Yes		Last entry in the visitors book + 6 years	SECURE DISPOSAL
2.2.8	Walking Bus registers	Yes		Date of register + 6 years	SECURE DISPOSAL

2.3 Human Resources					
	Basic file description	Personal Information	Statutory provisions	Retention period	Action at end of the administrative life of the record
Recruitment					
2.3.1	All records leading up to the appointment of a headteacher	Yes		Unsuccessful applicants – Date of appointment + 6 months. Otherwise retain in personnel file until end of appointment + 6 years (or + 15 years in cases of negligence or claims of child abuse)	SECURE DISPOSAL
2.3.2	All records leading up to the appointment of a member of staff/governor – unsuccessful candidates	Yes		Date of appointment of successful candidate + months	SECURE DISPOSAL
2.3.3	Pre-employment vetting information DBS checks – successful candidates	Yes	DBS Update Service Employer Guide 2014; Keeping Children Safe in Education 2018 Sections 73,74	For the duration of employment + 6 years	SECURE DISPOSAL
2.3.4	Forms of proof of identity taken for	Yes		Where possible complete using online system, if copies are taken	SECURE DISPOSAL

	DBS checks			retain in personnel file.	
2.3.5	Pre-employment vetting information- Evidence of the right to work in the UK– successful candidates	Yes	An employer's guide to the right to work Checks (Home Office, May 2015)	Retain in personnel file and retained until termination of employment + 6 years	SECURE DISPOSAL
Operational Staff Management					
2.3.6	Staff personnel file	Yes	Limitation Act 1980 (Section 2)	Retain in personnel file and retained until termination of employment + 6 years	SECURE DISPOSAL
2.3.7	Annual appraisal records	Yes		Current year + 6 years	SECURE DISPOSAL
2.3.8	Sickness absence monitoring	Yes		Sensitive data – keep separate from accident records. If sick pay not paid then current year + 3 years, otherwise current year + 6 years	SECURE DISPOSAL
2.3.9	Staff training – where leads to professional development	Yes		Length of time required by the professional body	SECURE DISPOSAL
2.3.10	Staff training e.g. first aid or health and safety	Yes		Retain in the personnel file as per point 2.3.6	SECURE DISPOSAL
2.3.11	Staff training relating to children e.g. safeguarding	Yes		Date of training + 40 years (in case of need to see records as part of an IICSA investigation)	SECURE DISPOSAL
Disciplinary and Grievance Processes					
2.3.12	Records relating to allegations of a child	Yes	Keeping children safe in education Statutory	Until normal retirement age or 10 years from the date of allegation	SECURE DISPOSAL

	protection nature against a member of staff		guidance for schools and colleges September 2018; Working together to safeguard children. A guide to inter-agency working to safeguard and promote the welfare of children 2018.	(whichever is the longer) then REVIEW.	
Note: The ACAS code of practice on disciplinary and grievance procedures recommends that the employee should be told how long a disciplinary warning will remain current. However, this does not mean that the data itself should be destroyed at the end of the set period. Any disciplinary proceedings data will be a record of an important event in the course of the employer's relationship with the employee. Should the same employee be accused of similar misconduct 5 years down the line, and then defend him or herself by saying "I would never do something like that" reference to the earlier proceedings may show that the comment should not be believed. Alternatively, if the employee were to be dismissed for some later offence and then claim at the tribunal that he or she had "fifteen years of unblemished service", the record of the disciplinary proceedings would be effective evidence to counter this claim. Employers should, therefore, be careful not to confuse the expiry of a warning for disciplinary proceedings with a requirement to destroy all reference to its existence in the personnel file. One danger is that the disciplinary procedure itself often gives the impression that, at the end of the effective period for the warning, the warning will be "removed from the file". This or similar wording should be changed to make it clear that, while the warning will not remain active in relation to future disciplinary matters, a record of what has occurred will be kept.					
2.3.13	Disciplinary proceedings	Yes			
	Oral warning			Date of warning + 6 months	SECURE DISPOSAL (if warnings are placed in personnel file 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 related to child protection then see above, otherwise dispose of at the conclusion of the case	SECURE DISPOSAL

Payroll and Pensions					
2.3.14	Absence record	Yes		Current year + 3 years	SECURE DISPOSAL
2.3.15	Income Tax form P60	Yes		Current year + 6 years	SECURE DISPOSAL
2.3.16	Maternity payment	Yes		Current year + 3 years	SECURE DISPOSAL
2.3.17	Overtime	Yes		Current year + 3 years	SECURE DISPOSAL
2.3.18	Payroll awards	Yes		Current year + 6 years	SECURE DISPOSAL
2.3.19	Personal bank details	Yes		Until superseded + 3 years	SECURE DISPOSAL
2.3.20	Sickness records	Yes		Current year + 3 years	SECURE DISPOSAL
2.3.21	Staff returns	Yes		Current year + 3 years	SECURE DISPOSAL
2.3.22	Time sheets	Yes		Current year + 3 years	SECURE DISPOSAL

2.4 **Health & Safety**					
	Basic file description	Personal Information	Statutory provisions	Retention period	Action at end of the administrative life of the record
2.4.1	Health and Safety policy statements			Life of policy + 3 years	SECURE DISPOSAL
2.4.2	Risk assessments			Life of risk assessment + 3 years	SECURE DISPOSAL
2.4.3	Accident reporting- - *Adults/Over 18 (all accidents)*	Yes	Social Security (Claims & Payments) Regulations 1979 Regulation 25. Social Security	The Accident Book- BI 510 – 3 years after last entry (i.e. if it takes 5 years to complete, the book must be retained for a further 3 years)	SECURE DISPOSAL

			Administration Act 1992 Section 8. Limitation Act 1980 Social Security (Claims & Payments) Regulations 1979. SI 1979 No 628 Social Security (Claims & Payments) Regulations SI 1987 No 1968 Revokes all but Part 1 of SI 1979 No 628 Social Security Administration Act 1992 Section 8. Social Security (Claims & Payments) Amendment (No 30 Regulations 1993 SI 1993 No 2113 Allows the information to be kept electronically	Completed pages must be kept secure with restricted access. DP Act 2018 and GDPR	
2.4.4	Accident reporting- - *Children (all accidents)*	Yes	As above	As above	SECURE DISPOSAL
2.4.5	Records relating to any reportable death, injury, disease or dangerous occurrence (RIDDOR)	Yes	Reporting of injuries, Diseases and Dangerous Occurrences and Regulations 2013 SI 2013 No 1471 Regulation 12(2)	Date of incident + 3 years provided that all records relating to the incident are held on the personnel file (see 2.4.2 above)	SECURE DISPOSAL
2.4.6	COSHH		COSSH Regulations 2002. SI 2002 No 2677 Regulation 11; Records kept under the 1994 and 1999 Regulations to be	Date of incident + 40 years	SECURE DISPOSAL

			kept as if the 2002 Regulations had not been made. Regulation 18 (2)		
2.4.7	Process of monitoring of areas where employees and persons are likely to have become in contact with asbestos		Control of Asbestos at Work Regulations 2012 SI 1012 No 632 Regulation 19.	Last action + 40 years	SECURE DISPOSAL
2.4.8	Process of monitoring of areas where employees and persons are likely to have come in contact with radiation	No	The Ionising Radiation Regulations 2017. SI 2017 No 1075 Regulation 11 As amended by SI 2018 No 390 Personal Protective Equipment (Enforcement\) Regulations 2018	2 years from the date of examination, records to include condition of equipment at the time of examination	SECURE DISPOSAL
2.4.9	Fire Precautions log books			Current year + 3 years	SECURE DISPOSAL
2.4.10	Health and Safety file showing current state of the building, including all alterations (wiring, plumbing, building works etc.) to be passed on in case of new ownership			Pass to new owner on sale or transfer of building	

2.5 Financial Management					
	Basic file description	Personal Information	Statutory provisions	Retention period	Action at end of the administrative life of the record
Risk Management and Insurance					
2.5.1	Employers Liability Insurance certificate			Closure of the school + 40 years (may be kept electronically)	SECURE DISPOSAL to be passed to the local authority if the school closes
Asset Management					
2.5.2	Inventories of furniture and equipment	Yes		Current year + 6 years	SECURE DISPOSAL
2.5.3	Burglary, theft and vandalism report forms	Yes		Current year + 6 years	SECURE DISPOSAL
Accounts and Statements (including budget management)					
2.5.4	Annual Accounts			Current year + 6 years	STANDARD DISPOSAL
2.5.5	Loans and grants managed by the school			Current year + 6 years	SECURE DISPOSAL
2.5.6	Process of All records relating to the creation of and management of budgets, including the annual budget statement and background papers	No		Life of the budget + 3 years	SECURE DISPOSAL

2.5.7	Invoices, receipts, orders, delivery notices			Current year + 6 years	SECURE DISPOSAL
2.5.8	Records relating to the collection and banking of monies			Current year + 6 years	
2.5.9	Records relating to the identification and collection of debt			Final payment of the debt + 6 years	
Pupil Finance					
2.5.11	Pupil premium Fund records	Yes		Date pupil leaves the provision + 6 years	SECURE DISPOSAL
Contract Management					
2.5.12	All records relating to the management of contracts under seal		Limitation Act 1980	Last payment on the contract + 12 years	SECURE DISPOSAL
2.5.13	All records relating to the management of contracts under signature		Limitation Act 1980	Last payment on the contract + 6 years	SECURE DISPOSAL
2.5.14	All records relating to the monitoring of contracts			Life of contract + 6 years	SECURE DISPOSAL
School Meals Management					
2.5.15	Free school meals	Yes		Current year + 6 years	SECURE DISPOSAL
2.5.16	School meals registers	Yes		Current year + 3 years	SECURE DISPOSAL

2.5.17	School meals summary sheets	Yes		Current year + 3 years	SECURE DISPOSAL
2.6 Property Management					
	Basic file description	Personal Information	Statutory provisions	Retention period	Action at end of the administrative life of the record
Property Management					
2.6.1	Title deeds of properties belonging to school			These should follow the property unless the property has been registered with Land Registry	
2.6.2	Plans of property belonging to school			These should be retained whilst the building belongs to the new school, then passed to the new owners if the building is leased or sold. See 2.4.10	
2.6.3	Leases of property leased by or to the school			Expiry of lease + 6 years	SECURE DISPOSAL
2.6.4	Records relating to the letting of school premises			Current financial year + 6 years	SECURE DISPOSAL
Maintenance					
2.6.5	All records relating to the maintenance of the school carried out by contractors			These should be retained whilst the building belongs to the new school, then passed to the new owners if the building is leased or sold. See 2.4.10	SECURE DISPOSAL
2.6.6	All records relating to the maintenance of the school carried			These should be retained whilst the building belongs to the new school, then passed to the new owners if the	SECURE DISPOSAL

	out by school employees, including maintenance log books			building is leased or sold. See 2.4.10	

3 **Pupil Management**					
	Basic file description	Personal Information	Statutory provisions	Retention period	Action at end of the administrative life of the record
3.1 Admissions Process					
3.1.1	All records relating to the creation and implementation of the School Admissions Policy		School Admissions Code Statutory guidance for admission authorities, governing bodies, local authorities, school adjudicators and admission appeals panels December 2014	Life of the policy + 3 years then review	SECURE DISPOSAL
3.1.2	Admissions – if the admission is successful	Yes	As above	Date of admission + 1 year	SECURE DISPOSAL
3.1.3	Admissions – if the appeal is unsuccessful	Yes	As above	Resolution of case + 1 year	SECURE DISPOSAL
3.1.4	Register of admissions		As above	Every entry in the admission register must be preserved for a period of 3 years after the date on which entry is made	
3.1.5	Proof of address supplied by parents as part of the	Yes	As above	Current year + 1 year	SECURE DISPOSAL

	admission process				
3.1.6	Supplementary information form including additional information such as religion, medical conditions etc.	Yes			
3.1.7	For successful admissions			This information should be added to the pupil file	SECURE DISPOSAL
3.1.7.1	For unsuccessful admissions			Until appeals process completed (GDPR)	SECURE DISPOSAL
3.2 Pupil's Educational Record					
3.2.1	Pupil's Educational Record required by The Education (Pupil Information) (England) Regulations 2005	Yes	The Education (Pupil Information) (England) Regulations 2005 SI 2005 No. 1437 As amended by SI 2018 No 688		
3.2.1.1	Primary			Retain whilst the child remains at the Primary School	The file should always follow the pupil
3.2.2	Examination results – pupil copies	Yes			
3.2.2.1	Internal			This information should be added to the pupil file	
3.2.3	Child protection information held on pupil file	Yes	"Keeping children safe in education Statutory guidance for schools and colleges 2018"; "Working together to safeguard children. A guide to inter-agency working to safeguard and promote	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. Note: These records will be subject to any instruction given by IICSA	

			the welfare of children"		
3.2.4	Child protection information held in separate files	Yes	As above	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 principle copy of this information will be found on the Local Authority Social Services record	SECURE DISPOSAL These records must be shredded
3.3 Attendance					
3.3.1	Attendance Registers	Yes	School Attendance: Departmental advice for maintained schools, Academies, independent schools and local authorities October 2014	Every entry in the attendance register must be preserved for a period of 3 years after the date of the entry.	SECURE DISPOSAL
3.3.2	Correspondence relating to any absence (authorised or unauthorised)	Potential	Education Act 1996 Section 7	Current academic year + 2 years	SECURE DISPOSAL
3.4 Special Educational Needs					
3.4.1	Special Educational Needs files, reviews and EHC Plans, including advice and information provided to parents regarding educational needs and accessibility strategy	Yes	Children and Family's Act 2014; Special Educational Needs and Disability Act 2001 Section 14	Date of birth of the pupil + 31 years	SECURE DISPOSAL

4 Curriculum and Extra Curricular					
4.1 Statistics and Management Information					
	Basic file description	Personal Information	Statutory provisions	Retention period	Action at end of the administrative life of the record
4.1.1	Curriculum returns	No		Current year + 3 years	SECURE DISPOSAL
4.1.2	Examination results (school copy)	Yes		Current year + 6 years	
4.1.2.1	*SATS records*	Yes			SECURE DISPOSAL
4.1.2.2	Results			The SATS results should be recorded in pupil files and will therefore be retained until the pupil reaches 25 years old. Composite records of whole year SATS results if kept should be retained for the current year + 6 years.	SECURE DISPOSAL
4.1.2.3	Examination papers			Retain until any appeals/validation process is complete	SECURE DISPOSAL
4.1.3	PAN reports	Yes		Current year + 6 years	SECURE DISPOSAL
4.1.4	Value Added and Contextual Data	Yes		Current year + 6 years	SECURE DISPOSAL
4.1.5	Self-evaluation forms	Yes			SECURE DISPOSAL
4.1.5.1	Internal moderation	Yes		Academic year + 1 academic year	SECURE DISPOSAL
4.1.5.2	External moderation	Yes		Until superseded	SECURE DISPOSAL
4.2 Implementation of curriculum					
	Basic file description	Personal Information	Statutory provisions	Retention period	Action at end of the administrative life of the record

4.2.1	Schemes of Work			Current year + 1 year	It may be appropriate to review these records at the end of each year and allocate a further retention period or SECURE DISPOSAL
4.2.2	Timetable			Current year + 1 year	
4.2.3	Class record books			Current year + 1 year	
4.2.4	Mark books			Current year + 1 year	
4.2.5	Record of homework set			Current year + 1 year	
4.2.6	Pupil's work			Where possible work should be returned to the pupil at the end of the academic year. Otherwise retain for Current year + 1 year	SECURE DISPOSAL
4.3 School Trips					
	Basic file description	Personal Information	Statutory provisions	Retention period	Action at end of the administrative life of the record
4.3.1	Parental consent forms for school trips where there has been NO major incident	Yes		Although the consent forms could be retained for date of birth + 22 years, the school can complete a risk assessment to assess whether the forms are likely to be required and could make a decision to dispose of the consent forms at the end of the trip (or at the end of the academic year) This is a pragmatic approach	SECURE DISPOSAL
4.3.2	Parental consent forms for school trips - where there	Yes	Limitation Act 1980 (Section 2)	Date of birth of the pupil involved in the incident + 25 years. The permission slips for	SECURE DISPOSAL

	has been a major incident			all the pupils on the trip need to be retained to show that the rules had been followed for all pupils.	
4.4 School Support Organisations					
	Basic file description	Personal Information	Statutory provisions	Retention period	Action at end of the administrative life of the record
Family Liaison Officer and Home School Liaison Assistants					
4.4.1	Day books	Yes		Current year + 2 years then review	SECURE DISPOSAL
4.4.2	Reports for outside agencies – where the report has been included on the case file created by the outside agency	Yes		Whilst the child is attending the school then destroy	SECURE DISPOSAL
4.4.3	Referral forms	Yes		While the referral is current	SECURE DISPOSAL
4.4.4	Contact data sheets	Yes		Current year then review, if no longer active then destroy	SECURE DISPOSAL
4.4.5	Contact data entries	Yes		Current year then review, if no longer active then destroy	SECURE DISPOSAL
4.4.6	Group registers	Yes		Current year + 2 years	SECURE DISPOSAL
Parent Teacher Associations					
4.4.7	Records relating to the creation and management of PTA's			Current year + 6 years then review	SECURE DISPOSAL

5 **Central Government**					
5.1 Local Authority					
	Basic file description	Personal Information	Statutory provisions	Retention period	Action at end of the administrative life of the record
5.1.1	Secondary transfer sheets (Primary)	Yes		Current year + 2 years	SECURE DISPOSAL
5.1.2	Attendance returns	Yes		Current year + 1 year	SECURE DISPOSAL
5.1.3	School census returns			Current year + 5 years	SECURE DISPOSAL
5.1.4	Circulars and other information sent from the local authority			Operational use	SECURE DISPOSAL
5.2 Central Government					
5.2.1	OFSTGED reports and papers where a physical copy is held			Life of the report then review	SECURE DISPOSAL
5.2.2	Returns made to central government			Current year + 6 years	SECURE DISPOSAL
5.2.3	Circulars and other information sent from central government			Operational use	SECURE DISPOSAL

Schedule of Records Destroyed/Deleted by Hundon and Thurlow Primary Federation

UNIQUE IDENTIFIER	FILE TITLE/BRIEF DESCRIPTION	DATE RANGE	NUMBER OF FILES	RETENTION SCHEDULE REF	AUTHORISING OFFICER	DATE OF APPROVAL FOR DISPOSAL	DATE DESTROYED	DISPOSAL METHOD	PLACE OF DISPOSAL	DESTORYING OFFICER/CONTRACTOR
