Park Hill Thorns Federation

Successful, confident learners. Responsible, compassionate individuals.

Data Protection Policy
Including Data Retention

(based on model by Legal Services 2018)

Written: June 2018

Agreed by governors: July 2025

Next review: June 2026

Changes Made – All highlighted in yellow

Contents

1. Aims

Park Hill Thorns Federation 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 (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:

- UK General Data Protection regulation (UKGDPR) – the EU GDPR was incorporated into the UK legislation, with some amendments, by The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2020 https://www.legislation.gov.uk/uksi/2020/1586/made
- Data Protection Act 2018 (DPA 2018) https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted

It is based on the guidance published by the Information Commissioner's Office (ICO) on the UK GDPR. https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/

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, 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 • Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes • 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.
Data Privacy Impact Assessment (DPIA)	Tools and assessments used to identify and reduce risks of a data processing activity. A DPIA can be carried out as part of Privacy by design and should be

	conducted for all major system or business change programmes involving the Processing of Personal Data.

4. The data controller

Park Hill Thorns Federation processes personal data relating to parents, pupils, staff, governors, volunteers, visitors and others, and therefore is a data controller.

Thorns Community Infant School and Park Hill Junior School are registered as a data controller with the ICO and will renew this registration annually or as otherwise legally required.

5. Roles and responsibilities

This policy applies to **all staff** employed by Park Hill Thorns Federation (Thorns Community Infant School and Park Hill Junior School), and to external organisations, volunteers and other 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 Park Hill Thorns Federation complies with all relevant data protection obligations.

5.2 Data Protection Officer

The data protection officer (DPO) is responsible for providing advice and guidance to the Federation in order to assist the Federation to implement this policy, monitor compliance with data protection law, and develop related policies and guidelines where applicable.

The DPO will carry out an annual audit of the Federation data processing activities and report to the Governing 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.

Our DPO is the **School DPO Service** and is contactable via schooldpo@warwickshire.gov.uk or alternatively;

School Data Protection Officer
Warwickshire Legal Services
Warwickshire County Council
Shire Hall
Market Square
Warwick
CV34 4RL

5.3 Headteacher

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

5.4 Data Protection Champions

The Federation has nominated the following individuals as designated persons to be contacted internally in relation to all matters relating to data protection issues, and to make referrals, where necessary, to the Data Protection Officer:

Rebecca Harrison, school business manager (SBM) who is contactable via harrison.r2@welearn365.com both schools

Lizzy Biggs who is contactable via head2307@welearn365.com Thorns and Park Hill

5.5 All staff

All members of 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 designated Data Protection Leads 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 UK GDPR is based on data protection principles that our Federation must comply with.

Park Hill Thorns Federations has adopted the principles to underpin its Data Protection Policy:

The principles require that all personal data shall be:

(1) processed lawfully, fairly and in a transparent manner ('lawfulness, fairness and transparency');

(2) used for specified, explicit and legitimate purposes ('purpose limitation');

(3) used in a way that is adequate, relevant and limited to what is necessary ('data minimisation');

(4) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, are erased or rectified without delay ('accuracy');

(5) kept no longer than is necessary ('storage limitation');

(6) processed in a manner that ensures it is safe and secure, ensuring that measures against unauthorised or unlawful processing and against accidental loss, destruction or damage are in place ('integrity and confidentiality').

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

7. Collecting personal data

7.1 Lawfulness, fairness and transparency

Park Hill Thorns Federation shall only process personal data where it has one of 6 'lawful bases' (legal reasons) available to the Federation 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 e.g. 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,** and carry out its official functions
- The data needs to be processed for the **legitimate interest** 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 which are set out in the UK GDPR and Data Protection Act 2018.

- The individual (or their parent/career when appropriate in the case of a pupil) has given **explicit consent**
- The data needs to be processed outperform 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 interest** of the individuals or another person, where the individual is physically or legally incapable of giving consent
- The data had already been made **manifestly public** by the individual
- The data needs to be processed 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 confidentially 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 historic 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/career 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 on 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.

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.

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 guidance set out in the Information and Records Management Society's toolkit for schools.

8. Sharing personal data

We will not normally share personal data with anyone else except as set out in the Federation's Privacy Notice. GDPR and the DPA 2018 also allow information to be shared 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 data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data we share
    - Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us

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

- The prevention or detection of crime and/or fraud
- The apprehension or prosecution of offenders
- The assessment or collection of tax owed to HMRC
- In connection with legal proceedings
- Where the disclosure is required to satisfy our safeguarding obligations
- Research and statistical purposes, as long as personal data is sufficiently anonymised or consent has been provided

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

The DPO will send the subject access request to the Data Protection Champion. If staff receive a subject access request they must immediately forward it to the Designated Data Protection Champions (SBM or Head of School), who will ensure that the DPO is informed.

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 person should have parental responsibility for the child, and 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 13 are generally not regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, subject access requests from parents or carers of pupils at our school [aged under 13] will in general be granted without requiring the express permission of the pupil.

These are not fixed rules 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
- 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 will not disclose information 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
- Is contained in adoption or parental order records
- Is given to a court in proceedings concerning the child

If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee which takes into account administrative costs.

A request will be deemed to be unfounded or excessive if it is repetitive, or asks for further copies of the same information.

When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO 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, where processing is based on the consent of the pupil or parent

- Ask us to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Object to processing which has been justified on the basis of public task, official authority or legitimate interests
- Challenge decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them)
- 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 Data Protection Champion who will send it to the DPO for information purposes.

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 physical or mental health of the pupil or another individual, or if tit would mean releasing exam marks before they are officially announced.

11. Biometric recognition systems

Not used within the Federation

12. CCTV

Not used within the Federation

13. Photographs and videos

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

The Federation 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.

Where the Federation need parental consent, it shall clearly explain how the photograph and/or video will be used to both the parent/carer and pupil. Where the Federation don't

need parental consent, it shall explain to the pupil how the photograph and/or video will be used.

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 parent/carers (or pupils where appropriate) have agreed to this.

Uses may include:

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

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

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

See our child protection and safeguarding policy and staff behavior policy for more information on our use of photographs and videos.

14. Data protection by design and default

The Federation shall put measures in place to show that it has integrated data protection into all of its 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)
- Consideration of whether a data protection impact assessment needs to be undertaken. The school will consider this if any of the following kinds of processing plan to be undertaken:
    - Use of systematic and extensive automated processing
    - Large scale processing of data, particularly where it involves special category or criminal offence data
    - Systematic monitoring of publicly accessible areas and any other form of surveillance
    - Processing of biometric or genetic data
    - Transfer of data outside of the European Economic Area
    - Profiling, evaluation or scoring
    - Automated decision making with legal or significant effects
    - Matching or combining datasets
    - Processing of data concerning vulnerable data subjects
    - Implementation of new technology or solutions

    - If processing would prevent a data subject from exercising a right or suing a service or contract

- On reviewing these criteria, if the school finds that the processing personal data presents a high risk to the rights and freedoms of individuals we will undertake a data protection impact assessment.
- 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
- Training members of staff on data protection law, this policy, any related policies and any other data protection matters; we will also keep a record of attendance
- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant
- Maintaining records of our processing activities, including:
    - For the benefit of data subjects, making available the name and contact details of our school and DPO and all information we are required to share about how we use and process their personal data (via our privacy notices)
    - For all personal data that we hold, maintaining an internal record of the type of data, data subject, how and why we are using the data, any third-party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure

15. Data security and storage of records

The Federation 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, pinned to notice/display boards, 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.
- Staff must ensure passwords are hard for anyone else to guess by incorporating numbers and mixed case into it.
- Encryption software is used to protect all portable devices and removable media on which personal information is stored, 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 the acceptable use agreement, staff and governor use of social media policy, staff handbook)

- 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)

16. 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, the Federation 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.

17. Personal data breaches

The Federation shall take all reasonable steps 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 1.

When appropriate, the Federation shall report the data breach to the ICO within 72 hours. Such breaches in the Federation 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

18. 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.

19. Links with other policies

This data protection policy is linked to our:

- Information Security Policy
- Data Retention
- Security Incidents and Breach Reporting Policy

Appendix 1: Personal data breach procedures

If staff become aware that information has not been handled according to procedures and there is a data breach or potential security incident, they must report it in accordance with this procedure.

When appropriate, the Federation will report the data breach to the ICO within 72 hours in accordance with the requirements of the GDPR.

1. Data protection breaches occur where personal data is lost, damaged, destroyed, stolen, misused and/or accessed unlawfully.

2. Examples of how a breach may occur include:

    a. Theft of data or equipment on which data is stored;
    b. Loss of data or equipment on which data is stored;
    c. Inappropriate access controls allowing unauthorised use;
    d. Accidental Loss;
    e. Destruction of personal data;
    f. Damage to personal data;
    g. Equipment failure;
    h. Unlawful disclosure of personal data to a third party;
    i. Human error;
    j. Unforeseen circumstances such as fire or flood;
    k. Hacking attack; or
    l. 'Blagging' offences where information is obtained by deceiving the organisation which holds it.

3. If any member of staff of the Federation, or Governor, discovers that data has been lost, or believes that there has been a breach of the data protection principles in the way that data is handled, you must immediately or no later than within 24 hours of first coming to notice, inform the Federation's Data Protection Champion.

4. Upon being notified, the Federation's Data Protection Champion will assess whether a breach of personal information has occurred, and the level of severity. If a breach has occurred but the risk of harm to any individual is low (for example, because no personal information has left the control of the Federation, then the Federation's Data Protection Champion will undertake an internal investigation to consider whether the Information Security Policy was followed, and whether any alterations need to be made to internal procedures as a result.

5. In all other cases, the incident must be notified to the Data Protection Officer immediately, who must follow the Information Commissioner's Office guidelines on notification and recording of the breach. The Data Protection Officer will provide advice and support on managing and responding to the data breach and advise whether they consider the incident to be reportable to the ICO. The priority must then be to close or contain the breach to mitigate / minimise the risks to those individuals affected by it.

All Thorns and Park Hill staff and Governors are expected to work in partnership with the Data Protection Champion and the Data Protection Officer in relation to the following matters

Notification of Breaches

Any member of staff or Governor who becomes aware of a personal information breach should provide full details to the Data Protection Champion for the Federation within 24 hours of being made aware of the breach. The Data Protection Champion will then complete the Data Breach Record Form and Incident Log. When completing the form details should be provided of the reporter's name, the date/time of the breach, the date/time of detecting the breach, and basic information about the type of breach and information about personal data concerned. Details of what has already been done to respond to the risks posed by the breach should also be included.

Containment and Recovery

The initial response is to investigate and contain the situation and a recovery plan including, damage limitation. You may need input from specialists such as IT, HR and legal and in some cases contact with external third parties.

- Seek assistance in the containment exercise. This could be isolating or closing a compromised section of the network, recovery of released documents, finding a lost piece of equipment or simply changing any related access codes
- Establish whether there is anything you can do to recover any losses and limit the damage the breach can cause.
- As well as the physical recovery of equipment, this could involve the use of backup records to restore lost or damaged data or ensuring that staff recognise when someone tries to use stolen data to access accounts.
- Consider whether any individual affected by the data breach should be notified

Assessing the Risks

Levels of risk can be very different and vary on an individual breach of data security depending what is lost/damaged/stolen. For example, if a case file is lost then risks are different depending on type of data and its sensitivity with potential adverse consequences for individuals. The Data Protection Champion should consider the following points:

- What type of data is involved?
- How sensitive is the data?
- If data has been lost or stolen, are there any protections in place such as encryption?
- What has happened to the data?
- If data has been stolen, could it be used for purposes which are harmful to the individuals to whom the data relate? If it has been damaged, this poses a different type and level of risk.
- Regardless of what has happened to the data, what could the data tell a third party about the individual? Sensitive data could mean very little to an opportunistic laptop thief while the loss of apparently trivial snippets of information could help a determined fraudster build up a detailed picture of other people
- How many individuals' personal data has been affected by the breach?
- Who are the individuals whose data has been breached?
- What harm can come to those individuals?
- Are there risks to physical safety or reputation, of financial loss or a combination of these and other aspects of their life?
- Are there wider consequences to consider such as a risk to life?
- Loss of public confidence in the Federation?

All staff and Governors should establish whether there is anything they can do to recover any losses and limit the damage the breach can cause.

Appendix 2: Appropriate Policy Document

1. About this policy

The Data Protection Act 2018 sets out the requirements to have an appropriate policy document when processing when processing special category data and criminal offence data.

To fulfil our duties and function as a Federation, we need to process personal information that is listed within Schedule 1 for the Data Protection Act 2018. Most of the processing within Schedule 1 of the Data Protection Act 2018 is required to have an appropriate policy document in place.

This is the appropriate policy document for Park Hill Thorns Primary Federation setting out how we will protect special categories of personal data and criminal convictions data.

2. Why we process Special Categories of Personal Data and Criminal Convictions Data

2.1 We process Special Categories of Personal Data and Criminal Convictions Data for the following purposes:

- 2.1.1 assessing an employee's fitness to work;
- 2.1.2 complying with health and safety obligations;
- 2.1.3 complying with the Equality Act 2010;
- 2.1.4 checking applicants' and employees' right to work in the UK;
- 2.1.5 verifying that candidate are suitable for employment or continued employment; and
- 2.1.6 To safeguard pupils, staff, and the community.
- 2.1.7 To support pupils, staff, and visitors who have a medical condition or disability.
- 2.1.8 To support pupils with special educational needs
- 2.1.9 TO meet our legal and ethical duties for the provision of education.

2.2 Where we process special categories of personal data and criminal convictions data, we will identify our lawful basis under both Article 6 and |Article 9 of the UK GDPR and, where appropriate, identify the condition with schedule 1 that allows for the processing.

2.3 Processing subject to Schedule 1 of the Data Protection Act 2018:

Processing condition for Special Categories of Personal Data	**Description of Processing**
Schedule 1, Part 1 – Conditions relating to employment, social security and social protection.	Processing data concerning health where we have duty outlined under employment law. Processing data concerning criminal convictions under Article 10 of the UK GDPR where we have a duty under employment law for recruitment, discipline, and dismissal. To comply with statutory guidance for safer recruitment. Processing information relating to Trade Union Membership to facilitate your right and

	preference to participate as a member of any trade union, and where there is industrial action that may impact the function of the school.
Schedule 1, Part 2 – Substantial Public Interest Conditions	**Statutory etc. And Government Purposes:** • Compliance with legal obligations and support the provision of education such as completing the school census, providing a common transfer file, to support pupils with medical conditions, to support pupils with special educational needs. • Compliance with legal obligations in connection with legal proceedings • We may also proceed criminal offence data under this condition.
	Equality of Opportunity and Treatment • To provide equal access to education • Compliance with legislation such as the Equality Act 2010. • To ensure equality of treatment.
	Preventing and detecting unlawful acts • To comply with our duty to safeguard pupils and the community. • To reduce risk to pupils, staff and visitors. • Sharing information with relevant and authorised agencies to support the prevention or investigations of unlawful acts.
	Protecting the Public against Dishonesty • Assisting other agencies in connection with regulatory requirements. • To protect and safeguarding pupils and the community.
	Support for Individuals with a Disability or Medical Condition • To ensure we keep pupils and staff safe. • To ensure all pupils can access education and other services in school. • To ensure our employees are properly supported and able to do their job.
	Counselling

	• To allow for individuals to access confidential counselling services as arranged through occupational health or other support services.
	Safeguarding of Children and Individuals at risk • To protect and safeguard pupils from physical and emotional harm, neglect or abuse. • To support the wellbeing of pupils at our school.
	Insurance • To process data that is required for insurance purposes.
	Occupational Pensions • To meet our legal obligation to provide a pension scheme for our workforce.
Schedule 1 , Part 3 – Additional Conditions Relating to Criminal Convictions, etc.	We process data criminal offence data for the purposes of recruitment and employment vetting. We may also process criminal offence data to protect and safeguard pupils, staff, and the community.

3. Personal data protection principles

3.1 The UK GDPR requires personal data to be processed in accordance with the six principles set out in Article 5(1). Article 5(2) required controllers to be able to demonstrate compliance with Article 5(1).

3.2 We comply with the principles relating to Processing of personal Data set out in the UK GDPR which require Personal Data to be:

3.2.1 Processed lawfully, fairly and in a transparent manner (Lawfulness, fairness and Transparency);

3.2.2 Collected only for specified, explicit and legitimate purposes (Purpose Limitation);

3.2.3 Adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed (Data Minimisation);

3.2.4 Accurate and where necessary kept up to date (Accuracy);

3.2.5 Not kept in a form which permits identification of Data Subjects for linger than is necessary for the purposes for which the data is Processed (Storage Limitation); and

3.2.6 Processed in a manner that manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful Processing and against accidental loss, destruction or damage (Security, Integrity and Confidentiality).

3.2.7 We are responsible for and must be able to demonstrate compliance with the data protection principles listed above (Accountability).

4. Compliance with data protection principles

4.1 Lawfulness, fairness and transparency

Personal Data must be processed lawfully, fairly and in a transparent manner in relation to the Data Subject.

We will only Process Personal Data fairly and lawfully and for specified purposes. The GUK GDPR restricts our actions regarding Personal Data to specified lawful purposes. We can Process Special Categories of Personal Data and Criminal Convictions data only if we have a legal ground for Processing and one of the specific Processing conditions relating to Special Categories of Personal Data or Criminal Convictions Data applies. We will identify and document the legal ground and specific Processing condition relied on for each Processing activity.

When collecting Special Categories of Personal Data and Criminal Convictions Data from Data Subjects, either directly from Data Subjects or indirectly (for example from a third party or publicly available source), we will provide Data Subjects with a Privacy Notice setting out all the information required by the UK GDPR which is concise, transparent, intelligible, easily accessible and in clear plain language which can be easily understood.

4.2 Purpose limitation

Personal Data must be collected only for specified, explicit and legitimate purposes. They must not be further Processed in any manner incompatible with those purposes.

We will only collect personal data for specified purposes and will inform Data Subjects what those purposes are in a published Privacy Notice. We will not use Personal Data for new, different, or incompatible purposes form those disclosed when it was first obtained unless we have informed the Data Subject of the new purposes and they have consented where necessary.

4.3 Data ministration

Personal Data shall be adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed. We will only collect or disclose the minimum Personal Data required for the purpose for which the data is collected or disclosed. We will ensure that we do no collect excessive data and that the Personal Data collected is adequate and relevant for the intended purposes.

4.4 Accuracy

Personal Data must be accurate and, where necessary, kept up to date. It must be corrected or deleted without delay when inaccurate.

We will ensure that the Personal Data we hold and use is accurate, complete, kept up to date, and relevant to the purpose for which it is collected by us. We check the accuracy of any Personal Data at the point of collection and at regular intervals afterwards. We take all reasonable steps to destroy or amend inaccurate or out-of-date- Personal Data.

4.5 Storage limitation

We only keep Personal Data in an identifiable form for as long as is necessary for the purposes for which it was collected, or where we have a legal obligation to do so. Once

we no longer need Personal Data it shall be deleted or rendered permanently anonymous.

We maintain a Data Retention Policy (Appendix 3) and related procedures to ensure Personal Data is deleted after a reasonable time has elapsed for the purposes for which it was being held, unless we are legally required to retain that data for longer.

We will ensure Data Subjects are informed of the period for which data is stored and how that period is determined in any applicable Privacy Notice.

4.6 Security, integrity, confidentially

Personal Data shall be Processed in a manner that ensures appropriate security of the Personal Data, including protection against unauthorised or unlawful Processing and against accidental loss destruction or damage, using appropriate technical or organisational measures.

We will implement and maintain reasonable and appropriate security measures against unlawful or unauthorised Processing of Personal Data and against the accidental loss of or damage to Personal Data.

4.7 Accountability principle

We are responsible for, and able to demonstrate compliance with these principles. Our DPO is responsible for ensuring that we are compliant with these principles. Any questions about this policy should be submitted to the DPO.

We will:

4.7.1 Ensure that records are kept of all Personal Data Processing activities, and that these are provided to the Information Commissioner on request.

4.7.2 Carry out a DPIA for any high-risk Personal Data Processing to understand how Processing may affect Data Subjects and consult the Information Commissioner if appropriate.

4.7.3 Ensure that a DPO is appointed to provide independent advice and monitoring of Personal Data handling, and that the DPO has access to report to the highest management level.

4.7.4 Have internal processes to ensure that Personal Data is only collected, used or handled in a way that is compliant with data protection law.

5. Controller's policies on retention and erasure of personal data

5.1 We take the security of Special Categories of Personal Data and Criminal Conviction Data very seriously. We have administrative, physical, and technical safeguards in place to protect Personal Data against unlawful or unauthorised Processing, or accidental loss or damage. We will ensure, where Special Categories of Personal Data or Criminal Convictions Data are Processed that:

5.1.1 The Processing is recorded, and the record sets out, where possible, a suitable time for the safe and permanent erasure of the different categories of data in accordance with our Data Retention Policy.

5.1.2 Where we no longer require Special Categories of Personal Data or Criminal Convictions Data for the purpose for which it was collected, we will delete it or render it permanently anonymous as soon as possible.

5.1.3 Where records are destroyed, we will ensure that they are safely and permanently disposed of.

5.2 Data Subjects receive a Privacy Notice setting out how their Personal Data will be handled when we first obtain their Personal Data, and this will include information on how we determine retention periods. The Privacy Notice is also available on the school websites.

6. Review

6.1 This policy on Processing Special Categories of Personal Data and Criminal Convictions Data is reviewed annually.

6.2 The policy will be retained where we process Special Categories of Personal Data and Criminal Convictions Data and for a period of a least six months after we stop carrying out such processing.

6.3 A copy of this policy will be provided to the Information Commissioner on request and free of charge.

Dated: July 2025
Next Review Date: July 2026

For further information:

For further information about our compliance with data protection law, please contact our Data Protection Lead (Harrison.r2@welearn365.com). Or our Data Protection Officer at the School DPR Service, Warwickshire Legal Service, Shire Hall, Warwick – Email schooldpo@warwickshire.gov.uk (when contacting our DPO, please state which school your query relates to).

Appendix 3

Data retention

The Park Hill Thorns Federation follows the retention schedule complied by IRMS (Information Records and Management Society) website link http://irms.org.uk/page/SchoolsToolkit.

This is policy will be reviewed on an annual basis in the first instance then every three years. Linked policies are:

- Security Policy
- General Data Protection Policy
- Online Safety Policy

NB "Secure Disposal" – this means disposal of confidential waste bins or if the school has the facility, shredding using a cross cut shredder

Table of Contents

1.1	Governing Body				
	Basic File Description	**Data Prot. Issues**	**Statutory Provisions**	**Retention Period (Operational)**	**Action at the end of the administrative life of the record**
1.1.1	Agendas for Governing Body meetings	There may be data protection issues if the meeting is dealing with confidential issues relating to staff		One copy should be retained with the master set of minutes. All other copies can be disposed of	SECURE DISPOSAL
1.1.2	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 Archive Service
	Inspection Copies (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)			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 retained with the signed set of minutes.
1.1.4	Meeting papers relating to the annual parents' meeting held under section 33 of the Education Act 2002	No	Education Act 2002, Section 33	Date of the meeting + a minimum of 6 years	SECURE DISPOSAL

1.1	Governing Body				
	Basic File Description	**Data Prot. Issues**	**Statutory Provisions**	**Retention Period (Operational)**	**Action at the end of the administrative life of the record**
1.1.5	Instrument 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 plan 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 the Governing Body	Yes		Date of the resolution of the complaint + a minimum of 6 years then review for further retention in case of contentious disputes	SECURE DISPOSAL
1.1.10	Annual Reports created under the requirements of the Education (Governor's Annual Reports) (England) (Amendment) Regulations 2002	No	Education (Governor's Annual Reports) (England) (Amendment) Regulations 2002 SI 2002 No 1171	Date of report + 10 years	SECURE DISPOSAL
1.1.11	Proposals concerning the change of status of a maintained school	No		Date proposal accepted or declined + 3 years	SECURE DISPOSAL

1.1	Governing Body				
	Basic File Description	**Data Prot. Issues**	**Statutory Provisions**	**Retention Period (Operational)**	**Action at the end of the administrative life of the record**
	including Specialist Status Schools and Academies				

1.2	Head Teacher and Senior Management Team				
	Basic File Description	**Data Prot. Issues**	**Statutory Provisions**	**Retention Period (Operational)**	**Action at the end of the administrative life of the record**
1.2.1	Log book 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 DISPSOAL
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 + 3 years then review	SECURE DISPSOAL
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 DISPSOAL
1.2.5	Correspondence created by head teachers, deputy head teachers,	There may be data protection issues if the		Date of correspondence + 3 years then review	SECURE DISPSOAL

1.2	Head Teacher and Senior Management Team				
	Basic File Description	**Data Prot. Issues**	**Statutory Provisions**	**Retention Period (Operational)**	**Action at the end of the administrative life of the record**
	heads of years and other members of staff with administrative responsibilities	correspondence refers to individual pupils or members of staff			
1.2.6	Professional Development Plans	Yes		Life of the plan + 6 years	SECURE DISPSOAL
1.2.7	School Development Plans	No		Life of the plan + 3 years	SECURE DISPSOAL

1.3	Admissions Process				
	Basic File Description	**Data Prot. Issues**	**Statutory Provisions**	**Retention Period (Operational)**	**Action at the end of the administrative life of the record**
1.3.1	All records relating to the creation and implementation of the School Admissions' Policy	No	School Admissions Code Statutory guidance for admission authorities, governing bodies, local authorities, schools adjudicators and admission appeals panels December 2014	Life of the policy +3 years then review	SECURE DISPOSAL
1.3.2	Admissions – if the admission is successful	Yes	School Admissions Code Statutory guidance for admission authorities, governing bodies, local authorities, schools adjudicators and admission appeals panels December 2014	Date of admission + 1 year	SECURE DISPOAL
1.3.3	Admissions – of the appeal is unsuccessful	Yes	School Admissions Code Statutory guidance for admission authorities, governing bodies, local authorities, schools adjudicators and admission appeals panels December 2014	Resolution of case + 1 year	SECURE DISPOSAL
1.3.4	Register of Admissions	Yes	School attendance: Departmental advice for maintained schools, academies, independent schools	Every entry in the admission register must be preserved for a period of	REVIEW Schools may wish to consider keeping the

1.3	**Admissions Process**				
	Basic File Description	**Data Prot. Issues**	**Statutory Provisions**	**Retention Period (Operational)**	**Action at the end of the administrative life of the record**
			and local authorities October 2014	three years after the date on which the entry was made (School attendance: Department advice for maintained schools, academies, independent schools and local authorities October 2014 p6)	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 Not Applicable	Yes		Current year + 1 year	SECURE DISPOSAL
1.3.6	Proofs of address supplied by parents as part of the admissions process	Yes	School Admissions Code Statutory guidance for admission authorities, governing bodies, local authorities, schools adjudicators and admission appeals panels December 2014	Current year + 1 year	SECURE DISPOSAL
1.3.7	Supplementary Information form including additional information such as religion, medical conditions etc.	Yes			
	For successful admissions			This information should be added to the pupil file	SECURE DISPOSAL
	For unsuccessful admissions			Until appeals process completed	SECURE DISPOSAL

1.4	Operational Administration				
	Basic File Description	**Data Prot. Issues**	**Statutory Provisions**	**Retention Period (Operational)**	**Action at the end of the administrative life of the record**
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 and pupils	No		Current year + 1 year	STANDARD DISPOSAL
1.4.4	Newsletters and other items with a short operational use	No		Current year + 1 year	STANDARD DISPOSAL
1.4.5	Visitors' Books and Signing in Sheets	Yes		Current year + 6 years then REVIEW	SECURE DISPOSAL
1.4.6	Records relating to the creation and management of Parent teacher Associations and/or Old Pupils Associations	No		Current year + 6 years then REVIEW	SECURE DISPOSAL

2. Human Resources

2.1	Recruitment				
	Basic File Description	**Data Prot. Issues**	**Statutory Provisions**	**Retention Period (Operational)**	**Action at the end of the administrative life of the record**
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 candidate	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	DBS Update Service Employer Guide June 2014: Keeping children safe in education. July 2015 (Statutory Guidance from Dept. of Education Sections 73, 74)	The school does not have to keep copies of DBS certificates. If the school does so the copy must NOT be retained for more than 6 months.	
2.1.5	Proofs of identity collected as part of the process of checking "portable" enhanced DBS disclosure	Yes		Where possible these should be checked and a note kept of what was seen and what has been checked. If it is felt necessary to keep copy documentation then this should be placed on the member of staff's personal file.	
2.1.6	Pre-employment vetting information – Evidence proving the right to work in the United Kingdom (Employers are required to take a "clear copy" of the	Yes	An employer's guide to right to work checks [Home Office May 2015]	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	

2.1	Recruitment				
	Basic File Description	**Data Prot. Issues**	**Statutory Provisions**	**Retention Period (Operational)**	**Action at the end of the administrative life of the record**
	documents which they are shown as part of this process)			for termination of Employment plus not less than two years	

2.2	Operational Staff Management				
	Basic File Description	**Data Prot. Issues**	**Statutory Provisions**	**Retention Period (Operational)**	**Action at the end of the administrative life of the record**
2.2.1	Staff Personal File	Yes	Limitation Act 1980 (Section 2)	Termination of Employment + 6 years	SECURE DISPOSAL
2.2.2	Timesheets	Yes		Current + 6 years	SECURE DISPOSAL
2.2.3	Annual appraisal/assessment records	Yes		Current + 6 years	SECURE DISPOSAL

2.3	Management of Disciplinary and Grievance Processes				
	Basic File Description	**Data Prot. Issues**	**Statutory Provisions**	**Retention Period (Operational)**	**Action at the end of the administrative life of the record**
2.3.1	Allegation of a child protection nature against a member of staff including where the allegation is unfounded (This review took place as the Independent Inquiry on Child Sexual Abuse was beginning. In light of this, it is recommended that all records relating to child abuse are retained until the Inquiry is completed. This section will then be reviewed again to take into account any recommendations the Inquiry might make concerning record retention)	Yes	"Keeping children safe in education Statutory guidance for schools and colleges March 2015";"working together to safeguard children. A guide to inter-agency working to safeguard and promote the welfare of children March 2015"	Until the person's normal retirement age of 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			

2.3	Management of Disciplinary and Grievance Processes				
	Basic File Description	**Data Prot. Issues**	**Statutory Provisions**	**Retention Period (Operational)**	**Action at the end of the administrative life of the record**
	Oral warning			Date of warning (Where the warning relates to child protection issues see above. If the disciplinary proceedings relate to a child protection matter please contact your Safeguarding Children Office for further advice) + 6 months	SECURE DISPOSAL [If warnings are placed on the personal file then they must be weeded from the file]
	Written warning – level 1			Date of warning + 6 months	
	Written warning – level 2			Date of warning + 12 months	
	Final warning			Date of warning + 18 months	
	Case not found			If the incident is child protection related then see above otherwise dispose of at the conclusion of the case	SECURE DISPOSAL

2.4	Health and Safety				
	Basic File Description	**Data Prot. Issues**	**Statutory Provisions**	**Retention Period (Operational)**	**Action at the end of the administrative life of the record**
2.4.1	Health and Safety Policy Statements	No		Life of the 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 t+ 12 years. In the case of serious accident a further retention period will need to be applied.	SECURE DISPOSAL
2.4.4	Accident Reporting	Yes	Social Security (Claims and Payments) Regulations 1979 Regulation 25. Social Security Administration Act 1992 Section 8. Limitation Act 1980		
	Adults			Date of incident + 6 years	SECURE DISPOSAL
	Children			DOB of the child + 25 years	SECURE DISPOSAL

2.4	Health and Safety				
	Basic File Description	**Data Prot. Issues**	**Statutory Provisions**	**Retention Period (Operational)**	**Action at the end of the administrative life of the record**
2.4.5	Control of Substances Hazardous to Health (COSHH)	No	Control of Substances Hazardous to Health Regulations 2002. SI 2002 No 2677 Regulation 11; Records kept under the 21994 and 1999 Regulations to be kept as if the 2002 Regulations had not been made. Regulation 18 (2)	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	Control of Asbestos at Work Regulations 2012 SI 1012 No 632 Regulation 19	Last action + 40 years	SECURE DISPOSAL
2.4.7	Process of monitoring of areas where employees and persons are likely to have become in contact with radiation	No		Last action + 50 years	SECURE DISPOSAL
2.4.8	Fire Precautions log books	No		Current year + 6 years	SECURE DISPOSAL

2.5	Payroll and Pensions				
	Basic File Description	**Data Prot. Issues**	**Statutory Provisions**	**Retention Period (Operational)**	**Action at the end of the administrative life of the record**
2.5.1	Maternity pay records	Yes	Statutory Maternity Pay (General) Regulations 1986 (SI1986/1960), revised 1999 (SI1999/567)	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

3.1	Risk Management and Insurance				
	Basic File Description	**Data Prot. Issues**	**Statutory Provisions**	**Retention Period (Operational)**	**Action at the end of the administrative life of the record**
3.11	Employer's Liability Insurance Certificate	No		Closure of the school + 40 years	SECURE DISPOSAL

3.2	Asset Management				
	Basic File Description	**Data Prot. Issues**	**Statutory Provisions**	**Retention Period (Operational)**	**Action at the end of the administrative life of the record**
3.2.1	Inventories of furniture and equipment	No		Current year + 6 years	SECURE DISPOSAL
3.2.2	Burglary, theft and vandalism report forms	No		Current year + 6 years	SECURE DISPOSAL

3.3	Accounts and Statements including Budget Management				
	Basic File Description	**Data Prot. Issues**	**Statutory Provisions**	**Retention Period (Operational)**	**Action at the end of the administrative life of the record**
3.3.1	Annual Accounts	No		Current year + 6 years	STANDARD DISPOSAL
3.3.2	Loans and grants managed by 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	Accounts and Statements including Budget Management				
	Basic File Description	**Data Prot. Issues**	**Statutory Provisions**	**Retention Period (Operational)**	**Action at the end of the administrative life of the record**
3.3.5	Invoice, receipts, order books and requisitions, delivery notices	No		Current financial year + 6 years	SECURE DISPOSAL
3.3.6	Records relating to the collection and banking of monies	No		Current financial year + 6 years	SECURE DISPOSAL
3.3.7	Records relating to the identification and collection of debt	NO		Current financial year + 6 years	SECURE DISPOSAL

3.4	Contract Management				
	Basic File Description	**Data Prot. Issues**	**Statutory Provisions**	**Retention Period (Operational)**	**Action at the end of the administrative life of the record**
3.4.1	All records relating to the management of contracts under seal	No	Limitation Act 1980	Last payment on the contract + 12 years	SECURE DISPOSAL
3.4.2	All records relating to the management of contracts under signature	No	Limitation Act 1980	Last payment on the contract + 6 years	SECURE DISPOSAL
3.4.3	Records relating to the monitoring of contracts	No		Current year + 2 years	SECURE DISPOSAL

3.5	School Fund				
	Basic File Description	**Data Prot. Issues**	**Statutory Provisions**	**Retention Period (Operational)**	**Action at the end of the administrative life of the record**
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

3.6	School Meals Management				
	Basic File Description	**Data Prot. Issues**	**Statutory Provisions**	**Retention Period (Operational)**	**Action at the end of the administrative life of the record**
3.6.1	Free School Meal 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

4.1	Property Management				
	Basic File Description	**Data Prot. Issues**	**Statutory Provisions**	**Retention Period (Operational)**	**Action at the end of the administrative life of the record**
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 of to the school	No		Expiry of the lease + 6 years	SECURE DISPOSAL
4.1.4	Records relating to the letting of school premises	No		Current financial year + 6 years	SECURE DISPOSAL

4.2	Maintenance				
	Basic File Description	**Data Prot. Issues**	**Statutory Provisions**	**Retention Period (Operational)**	**Action at the end of the administrative life of the record**
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	Maintenance				
	Basic File Description	**Data Prot. Issues**	**Statutory Provisions**	**Retention Period (Operational)**	**Action at the end of the administrative life of the record**
4.2.2	All records relating to the maintenance of the school carried out by school employees including maintenance books	No		Current year + 6 years	SECURE DISPOSAL

5. Pupil Management

5.1	Pupil Management				
	Basic File Description	**Data Prot. Issues**	**Statutory Provisions**	**Retention Period (Operational)**	**Action at the end of the administrative life of the record**
5.1.1	Pupils' Educational Record required by the Education (Pupil Information) (England) Regulations 2005	Yes	The Education (Pupil Information) (England) Regulations 2005 SI 2005 No. 1437		
	Primary			Retain whilst the child remains at the Primary School	The file should follow the pupil when he/she leaves the primary school. This will include: • To another primary school • To a secondary school • To a pupil referral unit • If the pupil dies whilst at the 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

5.1	Pupil Management				
	Basic File Description	**Data Prot. Issues**	**Statutory Provisions**	**Retention Period (Operational)**	**Action at the end of the administrative life of the record**
					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
	Secondary – not applicable		Limitation Act 1980 (Section 2)	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	
This review took place as the Independent Inquiry on Child Sexual Abuse was beginning. In light of this, it is recommended that all records relating to child abuse are retained until the Inquiry is completed. This section will then be reviewed again to take into account any recommendations the Inquiry might make concerning record retention					
5.1.3	Child Protection information held on pupil file	Yes	"Keeping children safe in education Statutory guidance for schools and colleges March 2015"; "Working together to safeguard children. A guide to inter-agency working to safeguard and promote the welfare of children March 2015"	If any records relating to child protection issues are placed on the pupil file.	SECURE DISPOSAL – these records MUST be shredded
5.1.4	Child Protection information held on separate files	Yes	"Keeping children safe in education Statutory guidance for schools and colleges March 2015"; "Working	DOB of the child + 25 years then review. This retention period was agreed in consultation with the	SECURE DISPOSAL – these records MUST be shredded

5.1	Pupil Management				
	Basic File Description	**Data Prot. Issues**	**Statutory Provisions**	**Retention Period (Operational)**	**Action at the end of the administrative life of the record**
			together to safeguard children. A guide to inter-agency working to safeguard and promote the welfare of children March 2015"	Safeguarding Children Group on the understanding that the principal copy of this information will be found on the Local Authority Social Services record	Information is passed to the new school and signature obtained on receipt of records; a copy of the transfer record is retained in school. The transfer record will be shredded at DOB of the child + 25 years.

5.2	Attendance				
	Basic File Description	**Data Prot. Issues**	**Statutory Provisions**	**Retention Period (Operational)**	**Action at the end of the administrative life of the record**
5.2.1	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 three years after the date on which the entry was made	SECURE DISPOSAL
5.2.2	Correspondence relating to authorized absence		Education Act 1996 Section 7	Current academic year + 2 years	SECURE DISPOSAL

5.3	Special Educational Needs				
	Basic File Description	**Data Prot. Issues**	**Statutory Provisions**	**Retention Period (Operational)**	**Action at the end of the administrative life of the record**
5.3.1	Special Educational Needs files, reviews and Individual Education Plans	Yes	Limitation Act 1980 (Section 2)	Date of Birth of the pupil + 25 years	REVIEW NOTE: This retention policy 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. Information is passed to the new school and signature obtained on receipt of records; a copy of the transfer record is retained in school. The transfer record will be shredded at DOB of the child + 25 years.
5.3.2	Statement maintained under section 234 of the Education Act 1990 and any amendments made to the statement	Yes	Education Act 1996 Special Educational Needs and Disability Act 2001 Section 1	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 Information is passed to the new school and signature obtained on receipt of records; a copy of the transfer record is

5.3	Special Educational Needs				
	Basic File Description	**Data Prot. Issues**	**Statutory Provisions**	**Retention Period (Operational)**	**Action at the end of the administrative life of the record**
					retained in school. The transfer record will be shredded at DOB of the child + 25 years.
5.3.3	Advice and information provided to parents regarding educational needs	Yes	Special Educational Needs and Disability Act 2001 Section 2	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 Information is passed to the new school and signature obtained on receipt of records; a copy of the transfer record is retained in school. The transfer record will be shredded at DOB of the child + 25 years.
5.3.4	Accessibility Strategy	Yes	Special Educational Needs and Disability Act 2001 Section 14	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 Information is passed to the new school and signature obtained on receipt of records; a copy of the transfer record is retained in school. The transfer record will be shredded at DOB of the child + 25 years.
5.4	**Images and video**				
	Basic File Description	**Data Prot. Issues**	**Statutory Provisions**	**Retention Period (operational)**	**Action at the end of the administrative life of the record**
5.4.1	Electronic photographs and video	Yes		Retain whilst the child remains at the Primary School	SECURE DISPOSAL

5.3	Special Educational Needs				
	Basic File Description	**Data Prot. Issues**	**Statutory Provisions**	**Retention Period (Operational)**	**Action at the end of the administrative life of the record**
				or where the image remains in use as part of an active school document eg school brochure, website	Except where an image is retained as part of a school archive in which case parental permission will be sought.

6. Curriculum Management

6.1	Statistics and Management Information				
	Basic File Description	**Data Prot. Issues**	**Statutory Provisions**	**Retention Period (Operational)**	**Action at the end of the administrative life of the record**
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			SECURE DISPOSAL
	Results			The SATS results should be recorded on the pupil's educational file and will therefore be retained until the pupil reaches the age of 25 years. The school may wish to keep a composite record of all the whole year SATs results. These could be kept for current year + 6 years to allow suitable comparison	SECURE DISPOSAL
	Examination Papers			The examination papers should be kept until any appeals/validation process is complete	SECURE DISPOSAL

6.1	Statistics and Management Information				
	Basic File Description	**Data Prot. Issues**	**Statutory Provisions**	**Retention Period (Operational)**	**Action at the end of the administrative life of the record**
6.1.3	Published Admission Number (PAN) Reports	Yes		Current year + 6 years	SECURE DISPOSAL
6.1.4	Value Added and Contextual Data	Yes		Current year + 6 years	SECURE DISPOSAL
6.1.5	Self-Evaluation Forms	Yes		Current year + 6 years	SECURE DISPOSAL

6.2	Implementation of Curriculum				
	Basic File Description	**Data Prot. Issues**	**Statutory Provisions**	**Retention Period (Operational)**	**Action at the end of the administrative life of the record**
6.2.1	Schemes of Work	No		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
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 of homework set	No		Current year + 1 year	
6.2.6	Pupil's Work	no		Where possible pupil's 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-Curricular Activities

7.1	Educational Visits outside the Classroom				
	Basic File Description	**Data Prot. Issues**	**Statutory Provisions**	**Retention Period (Operational)**	**Action at the end of the administrative life of the record**
7.1.1	Records created by schools to obtain approval to run an Educational Visit outside the Classroom – Primary Schools	No	Outdoor Education Advisers' Panel National Guidance website http://oeapng.info specifically Section 3 – "Legal Framework and Employer	Date of visit + 14 years	SECURE DISPOSAL

7.1	Educational Visits outside the Classroom				
	Basic File Description	**Data Prot. Issues**	**Statutory Provisions**	**Retention Period (Operational)**	**Action at the end of the administrative life of the record**
			Systems" and Section 4 – "Good Practice".		
7.1.2	Records created by schools to obtain approval to run an Educational Visit outside the Classroom – Primary Schools – Not applicable	No	Outdoor Education Advisers' Panel National Guidance website http://oeapng.info specifically Section 3 – "Legal Framework and Employer Systems" and Section 4 – "Good Practice".	Date of visit + 10 years	SECURE DISPOAL
7.1.3	Parental consent forms for school trips where there has been no major incident	Yes		Conclusion of trip	Although consent forms could be retained for DOB + 22 years, the requirement for them being needed I 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 consent forms for school trips where there has been a major incident	Yes	Limitation Act 1980 (Section2)	DOB of the pupil involved in the incident + 25 years The permission slips for all the pupils on the trip need to be retained to show that the rules had been followed for all pupils	

7.2	Walking Bus				
	Basic File Description	**Data Prot. Issues**	**Statutory Provisions**	**Retention Period (Operational)**	**Action at the end of the administrative life of the record**
7.2.1	Walking Bus Registers	Yes		Date of register + 3 years 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	SECURE DISPOSAL [If these records are retained electronically any back-up copies should be destroyed at the same time]

7.3	Family Liaison Officers and Home School Liaison Assistants				
	Basic File Description	**Data Prot. Issues**	**Statutory Provisions**	**Retention Period (Operational)**	**Action at the end of the administrative life of the record**
2.1.1	Day Books	Yes		Current year + 2 years then review	
2.1.2	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	
2.1.3	Referral forms	Yes		Whilst the referral is current	
2.1.4	Contact data sheets	Yes		Current year then review, if contact is no longer active then destroy	
2.1.5	Contact database entries	Yes		Current year then review, if contact is no longer active then destroy	
2.1.6	Group Registers	YEs		Current year + 2 years	

8. Central Government and Local Authority

8.1	Local Authority				
	Basic File Description	**Data Prot. Issues**	**Statutory Provisions**	**Retention Period (Operational)**	**Action at the end of the administrative life of the record**
8.1.1	Secondary Transfer Sheet (Primary)	Yes		Current year + 2 years	SECURE DISPOSAL
8.1.2	Attendance Returns	Yes		Current year + 1 year	SECURE DISPOSAL
8.1.3	School Census Returns	No		Current year + 5 years	SECURE DISPOSAL
8.1.4	Circulars and other information sent from the Local Authority	NO		Operational use	SECURE DISPOSAL

8.2	Central Government				
	Basic File Description	**Data Prot. Issues**	**Statutory Provisions**	**Retention Period (Operational)**	**Action at the end of the administrative life of the record**
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		Operation use	SECURE DISPOSAL