THE LION WORKS SCHOOL POLICY

GDPR and Data Protection Policy

Author of policy and position of responsibility: Justine Collinson, Headteacher	**Date policy finalised** September 2024
Approved by: Sarah Rempel, Director of Education	**Date of approval** September 2024
Due to be reviewed: July 2025	**Date of review:**

Contents

Context

The Lion Works School is an Independent special school. We are part of an ethical and progressive organisation that believes it can achieve real change for children, young people and their families.

The Lion Works School is situated within the BCP local authority. We offer an academic and vocational specialist learning provision across KS3, KS4 and Post 16 aiming to reduce barriers to enable successful learning experiences and outcomes. There are a variety of routes a student can take, which include GCSEs, BTECs and other accredited qualifications whilst building confidence, improving wellbeing, enabling self-regulation and increasing attendance. Our school is full of life and has a wealth of resources to spark interest and ignite that passion to achieve, equipping our students for everyday life and the opportunities that await them.

We adhere to the values of **ARC**:

Ambition
Resilience
Community

The Lion Works School operates within the SPELL framework. SPELL is The National Autistic Society's framework for understanding and responding to the needs of children and adults on the autism spectrum. It focuses on five principles that have been identified as vital elements of best practice in autism and emphasises ways to change the environment and our approaches to meet the specific needs of each person.

SPELL stands for Structure, Positive approaches and expectations, Empathy, Low arousal, Links:

Structure	Structure makes the world a more predictable, accessible and safer place. We can support people on the autism spectrum in creating structured environments using visual information.
Positive (approaches and expectations)	We must seek to establish and reinforce self-confidence and self-esteem by building on natural strengths, interest and abilities.
Empathy	We must try to see the world from the standpoint of the autistic child or adult, knowing what it is that motivates or interests them but importantly what may also frighten, preoccupy or otherwise distress them.
Low arousal	Approaches and the environment need to be calm and ordered in such a way so as to reduce anxiety and aid concentration.
Links	Autistic people, their parents or advocates should be seen as partners. Open links and communication will reduce the risk of misunderstanding, confusion or the adoption of fragmented, piecemeal approaches.

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 UK data protection law. This policy is intended to ensure that personal information is dealt with properly and securely and in accordance with the legislation. It will apply to personal information regardless of the way it is used, recorded and stored and whether it is held in paper files or electronically.

Legislation and Guidance

General Data Protection Regulation (GDPR) and The Data Protection Act 2018 (DPA) is the law that protects personal privacy and upholds individual's rights. It applies to anyone who handles or has access to people's personal data. This policy meets the requirements of:

- UK General Data Protection Regulation (UK GDPR) – the EU GDPR was incorporated into UK Legislation with some amendments by The Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2020
- Data Protection Act 2018 (DPA 2018)

This policy is based on guidance published by the Information Commissioner's Office (ICO) on the UK GDPR. It also reflects the ICO's guidance for the use of surveillance camera and personal information.

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

	• 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.

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 with the ICO and has paid its data protection fee to the ICO, as legally required.

Roles and Responsibilities

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 school 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. Our DPO is HR Manager, **Caroline Chadwick** and is contactable via email at **caroline@thelionworksschool.org**

Headteacher

The headteacher may act as the Data controller on a day-to-day basis or may delegate this responsibility to another member of staff with explicit agreement of the board.

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 they have a lawful basis to use personal data in a particular way
    - If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the UK
    - If there has been a data breach
    - Whenever they are engaging in a new activity that may affect the privacy rights of individuals
    - If they need help with any contracts or sharing personal data with third parties

Data Protection Principles

The UK 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.

Collecting Personal Data

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 can **perform a task in the public interest or exercise its statutory obligations**
- The data needs to be processed for the **legitimate interests** of the school (where the processing is not for any tasks the school performs) or a third party, provided the individual's rights and freedoms are not overridden
- The individual (or their parent/carer/guardian 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/guardian 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/guardian 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.

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.

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/guardian that puts the safety of our staff at risk
- We need to take steps to safeguard the individual whose data is shared or safeguard another individual but in doing so the data of another must be shared with an appropriate agency
- We need to liaise with other agencies – we will seek consent as necessary before doing this
- Our suppliers or contractors need data to enable us to provide services to our staff and pupils – for example, IT companies. When doing this, we will:
    - Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with UK data protection law.
    - Establish a contract with the supplier or contractor to ensure the fair and lawful processing of any personal data we share
    - Only share data that the supplier or contractor needs to carry out their service

We will also share personal data with law enforcement and government bodies where we are legally required to do so. We may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of our pupils or staff. Where we transfer personal data internationally, we will do so in accordance with UK data protection law.

Subject Access Requests and other Rights of Individuals

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 in any form, they must immediately forward it to the DPO.

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.

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.

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.

Parental Requests to see Educational Records

Parents, or those with parental responsibility, do not have an automatic parental right of access to the educational record held in our independent school setting, but we do choose to provide access to your child's educational record (which includes most information about a pupil). This right applies as long as the pupil 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. To make a request, please contact the Headteacher.

CCTV

We use CCTV in various locations around the school site to ensure it remains safe. We will follow the ICO's guidance for the use of CCTV, and comply with data protection principles. We do not need to ask individuals' permission to use CCTV, but we make it clear where individuals are being recorded. There are signs explaining that CCTV is in use. Any enquiries about the CCTV system should be directed to Justine Collinson, our Headteacher.

Photographs and Videos

As part of our school activities, we may take photographs and record images of individuals within our school. We will obtain written consent from parents/carers for photographs and videos to be taken of their child for communication, marketing, and promotional materials. We will clearly explain how the photograph and/or video will be used to both the parent/carer/guardian 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. When using photographs and videos in this way we will not accompany them with any other personal information about the child, to ensure they cannot be identified.

Data Protection by Design and Default

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

- Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge.
- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law (see section 6)
- Completing data protection impact assessments where the school's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on this process)
- Integrating data protection into internal documents including this policy, any related policies and privacy notices
- Regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters; we will also keep a record of attendance
- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant
- Appropriate safeguards being put in place if we transfer any personal data outside of the UK, where different data protection laws may apply
- Maintaining records of our processing activities, including:
    - For the benefit of data subjects, making available the name and contact details of our school and DPO and all information we are required to share about how we use and process their personal data (via our privacy notices)

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

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
- Staff are required to change passwords for school email accounts at least once per term
- All portable devices and removable media are password protected, 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 ICT and Internet Acceptable Use 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)

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.

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 1.

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 or those 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

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.

Monitoring Arrangements

The DPO is responsible for monitoring the implementation of this policy. The Headteacher is responsible, unless it has been delegated with written agreement of the board, for day to day adherence to this policy. The policy will be reviewed annually and approved by the school board.

Links with other Policies

This policy is linked to our:

- Safeguarding and child protection policy
- ICT and Internet acceptable use policy
- Staff code of conduct
- Privacy notices

Appendix 1 - Personal Data Breach Procedure

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

- On finding or causing a breach, or potential breach, the staff member, governor or data processor must immediately notify the data protection officer (DPO) by filling out and submitting a 'Data breach reporting form'.
- 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.
- Staff and board members will cooperate with the investigation (including allowing access to information and responding to questions). The investigation will not be treated as a disciplinary investigation
- If a breach has occurred or it is considered to be likely that is the case, the DPO will alert the school board
- The DPO will make all reasonable efforts to contain and minimise the impact of the breach. Relevant staff members or data processors should help the DPO with this where necessary, and the DPO should take external advice when required (e.g., from IT providers). (See the actions relevant to specific data types at the end of this procedure)
- The DPO will assess the potential consequences (based on how serious they are and how likely they are to happen) before and after the implementation of steps to mitigate the consequences
- The DPO will work out whether the breach must be reported to the ICO and the individuals affected using the ICO's self-assessment tool
- The DPO will document the decisions (either way), in case the decisions are challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored on the school's computer system in a dedicated Data Protection folder.
- Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website, or through its breach report line (0303 123 1113), within 72 hours of the school's awareness of the breach. As required, the DPO will set out:
    - A description of the nature of the personal data breach including, where possible:
        - The categories and approximate number of individuals concerned.
        - The categories and approximate number of personal data records concerned.
        - The name and contact details of the DPO

- A description of the likely consequences of the personal data breach
- A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned

- If all the above details are not yet known, the DPO will report as much as they can within 72 hours of the school's awareness of the breach. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible.
- Where the school is required to communicate with individuals whose personal data has been breached, the DPO will tell them in writing. This notification will set out:
    - A description, in clear and plain language, of the nature of the personal data breach
    - The name and contact details of the DPO.
    - A description of the consequences of the personal data breach
    - A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned
- The DPO will consider, in light of the investigation and any engagement with affected individuals, whether to notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies
- The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:
    - Facts and cause
    - Effects
    - Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)

Records of all breaches will be stored on the school's computer system in a dedicated Data Protection folder.

The DPO/Headteacher and School Board will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible. The DPO/Headteacher and School Board will meet at least twice a year to assess recorded data breaches and identify any trends or patterns requiring action by the school to reduce risks of future breaches

Actions to minimise the impact of data breaches

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

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 our external IT support provider to attempt to recall it from external recipients and remove it from the school's email system (retaining a copy if required as evidence)
- In any cases where the recall is unsuccessful or cannot be confirmed as successful, the DPO will consider whether it 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 School Board and discuss whether the school should inform any, or all, of its 3 local safeguarding partners.

Appendix 2 - Data Incident and Breach Report Form

This form is to be used when reporting a **suspected data breech.** Please complete all relevant fields on page 1&2 of this document before submitting it the Data Protection Officer (caroline@thelionworksschool.org)

Incident Overview:		
Reported by:		
Email Address:	Date:	Time:
Did the person reporting the incident also discover it? Y/N		
If no – Who did discover it?		
Who has this been reported to?		

Incident details			
Description of Incident: (including what went wrong and what happened, include what data has been breached, individuals concerned and any other relevant information)			
How did you find about the incident?			
Date Incident discovered		Time:	
Date incident reported		Time:	

Type of Breach (please tick the relevant type	
Confidentiality: This is where there is an unauthorised or accidental disclosure of, or access to personal data.	

If there has been any delay in reporting this incident, please explain why

Number of records involved in the incident	
How many data subjects could be affected	

Categories of data subjects affected (tick all that apply)					
Staff		Employees of other organisations		Contractors/Advisors/ Consultants	
Parents/Carers		Governors		Students	
Other (give details)					

Availability: This is where there is accidental or unauthorised loss of access to, or destruction of personal data	
Integrity: This is where there is an unauthorised or accidental alteration of personal data	

Action taken:		
Has the lost/disclosed data been recovered	Fully	Partially
Describe the actions you have taken, propose to take as a result of the incident: (e.g., review working practices, taken necessary steps to retrieve data etc)		
Any further action required:		

Signed	
Print Name	
Date	

Appendix 3 – Data Destruction Schedule (to be completed once annually)

Completion page

School name: _____

Review completed by: _____

Date: _____

Approved by Headteacher: _____

Date: _____

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

A. Summary of areas reviewed:

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

1. Management of the School

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

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

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

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

1.1 Governing Body (continued…)					
Ref	**Basic file description**	**Data Protection Issues**	**Retention Period [Operational]**	**Action at the end of the administrative life of the record**	**Annual Review Completed Tick (√)**
1.1.6	Action plans created and administered by the Governing Body	No	Life of the action plan + 3 years	SECURE DISPOSAL	
1.1.7	Policy documents created and administered by the Governing Body	No	Life of the policy + 3 years	SECURE DISPOSAL	
1.1.8	Records relating to complaints dealt with by the Governing Body	Yes	Date of the resolution of the complaint + a minimum of 6 years then review for further retention in case of contentious disputes	SECURE DISPOSAL	

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

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

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

1.3.9	For unsuccessful admissions		Until appeals process completed	SECURE DISPOSAL	

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

2. Human Resources

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

2.1 Recruitment					
Ref	**Basic file description**	**Data Protection Issues**	**Retention Period [Operational]**	**Action at the end of the administrative life of the record**	**Annual Review Completed Tick (√)**
2.1.1	All records leading up to the appointment of a new headteacher	Yes	Date of appointment + 6 years	SECURE DISPOSAL	
2.1.2	All records leading up to the appointment of a new member of staff – unsuccessful candidates	Yes	Date of appointment of successful candidate + 6 months	SECURE DISPOSAL	
2.13	All records leading up to the appointment of a new member of staff – successful candidate	Yes	All the relevant information should be added to the staff personal file (see below) and all other information retained for 6 months	SECURE DISPOSAL	
2.1.4	Pre-employment vetting information – DBS Checks	No	The school does not have to keep copies of DBS certificates. If the school does so the copy must NOT be retained for more than 6 months		
2.1.5	Proofs of identity collected as part of the process of checking "portable" enhanced DBS disclosure	Yes	Where possible these should be checked and a note kept of what was seen and what has been checked. If it is felt necessary to keep copy documentation then this should be placed on the member of staff's personal file		
2.1.6	Pre-employment vetting information – Evidence proving the right to work in the United Kingdom[4]	Yes	Where possible these documents should be added to the Staff Personal File [see below], but if they are kept separately then the Home Office requires that the documents are kept for termination of Employment plus not less than two years		

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

2.3 Management of Disciplinary and Grievance Processes					
Ref	**Basic file description**	**Data Protection Issues**	**Retention Period [Operational]**	**Action at the end of the administrative life of the record**	**Annual Review Completed Tick (√)**
2.3.1	Allegation of a child protection nature against a member of staff including where the allegation is unfounded[5]	Yes	Until the person's normal retirement age or 10 years from the date of the allegation whichever is the longer then REVIEW. Note allegations that are found to be malicious should be removed from personnel files. If found they are to be kept on the file and a copy provided to the person concerned	SECURE DISPOSAL These records must be shredded	
2.3.2	Disciplinary Proceedings	Yes			
2.3.3	oral warning		Date of warning + 6 months	SECURE DISPOSAL [If warnings are placed on personal files then they must be weeded from the file]	
2.3.4	written warning – level 1		Date of warning + 6 months		
2.3.5	Support plan		Date of warning + 12 months		
2.3.6	final warning		Date of warning + 18 months		
2.3.7	case not found		If the incident is child protection related then see above otherwise dispose of at the conclusion of the case	SECURE DISPOSAL	

2.4 Health and Safety					
Ref	**Basic file description**	**Data Protection Issues**	**Retention Period [Operational]**	**Action at the end of the administrative life of the record**	**Annual Review Completed Tick (√)**
2.4.1	Health and Safety Policy Statements	No	Life of policy + 3 years	SECURE DISPOSAL	
2.4.2	Health and Safety Risk Assessments	No	Life of risk assessment + 3 years	SECURE DISPOSAL	
2.4.3	Recordsrelatingto accident/ injury atwork	Yes	Date of incident + 12 years In the case of serious accidents a further retention period will need to be applied	SECURE DISPOSAL	
2.4.4	Accident Reporting	Yes			
2.4.5	Adults		Date of the incident + 6 years	SECURE DISPOSAL	
2.4.6	Children		DOB of the child + 25 years	SECURE DISPOSAL	
2.4.7	Control of Substances Hazardous to Health (COSHH)	No	Current year + 40 years	SECURE DISPOSAL	
2.4.8	Process of monitoring of areas where employees and persons are likely to have become in contact with asbestos	No	Last action + 40 years	SECURE DISPOSAL	
2.4.9	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	
2.4.10	Fire Precautions log books	No	Current year + 6 years	SECURE DISPOSAL	

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

3. Financial Management of the School

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

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

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

3.3 Accounts and Statements including Budget Management					
Ref	**Basic file description**	**Data Protection Issues**	**Retention Period [Operational]**	**Action at the end of the administrative life of the record**	**Annual Review Completed Tick (√)**
3.3.1	Invoices, receipts, order books and requisitions, delivery notices	No	Current financial year + 6 years	SECURE DISPOSAL	

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

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

4. Property Management

This section covers the management of buildings and property.

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

5. Pupil Management

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

5.1 Pupil's Educational Record					
Ref	**Basic file description**	**Data Protection Issues**	**Retention Period [Operational]**	**Action at the end of the administrative life of the record**	**Annual Review Completed Tick (√)**
5.1.1	Pupil's Educational Record required by The Education (Pupil Information) (England) Regulations 2005	Yes			
5.1.2	Primary		Retain whilst the child remains at the primary school	The file should follow the pupil when he/she leaves the primary school. [3]	
5.1.3	Secondary		Date of Birth of the pupil + 25 years	SECURE DISPOSAL	
5.1.4	Examination Results – Pupil Copies	Yes			
5.1.5	Public		This information should be added to the pupil file	All uncollected certificates should be returned to the examination board.	
5.1.6	Internal		This information should be added to the pupil file		
5.1.7	Child Protection information held on pupil file		If any records relating to child protection issues are placed on the pupil file, it should be in a sealed envelope and then retained for the same period of time as the pupil file.	SECURE DISPOSAL – these records MUST be shredded	
5.1.8	Child protection information held in separate files		DOB of the child + 25 years then review This retention period was agreed in consultation with the Safeguarding Children Group on the understanding that the principal copy of this information will be found on the Local Authority Social Services record	SECURE DISPOSAL – these records MUST be shredded	

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

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

5.3 Special Educational Needs					
Ref	**Basic file description**	**Data Protection Issues**	**Retention Period [Operational]**	**Action at the end of the administrative life of the record**	**Annual Review Completed Tick (√)**
5.3.1	Special Educational Needs files, reviews and Individual Education Plans	Yes	Date of Birth of the pupil + 25 years	REVIEW NOTE: This retention period is the minimum retention period that any pupil file should be kept. Some authorities choose to keep SEN files for a longer period of time to defend themselves in a "failure to provide a sufficient education" case. There is an element of business risk analysis involved in any decision to keep the records longer than the minimum retention period and this should be documented.	
5.3.2	Statement maintained under section 234 of the Education Act 1990 and any amendments made to the statement	Yes	Date of birth of the pupil + 25 years [This would normally be retained on the pupil file]	SECURE DISPOSAL unless the document is subject to a legal hold	
5.3.4			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	
5.3.5			Date of birth of the pupil + 25 years [This would normally be retained on the pupil file]	SECURE DISPOSAL unless the document is subject to a legal hold	

6. Curriculum Management

6.1 Statistics and Management Information					
Ref	**Basic file description**	**Data Protection Issues**	**Retention Period [Operational]**	**Action at the end of the administrative life of the record**	**Annual Review Completed Tick (√)**
6.1.1	Curriculum returns	No	Current year + 3 years	SECURE DISPOSAL	
6.1.2	Examination Results (Schools Copy)	Yes	Current year + 6 years	SECURE DISPOSAL	
6.1.3	SATS records –	Yes			
6.1.4	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	
6.1.5	Examination Papers		The examination papers should be kept until any appeals/validation process is complete	SECURE DISPOSAL	
6.1.6	Published Admission Number (PAN) Reports	Yes	Current year + 6 years	SECURE DISPOSAL	
6.1.7	Value Added and Contextual Data	Yes	Current year + 6 years	SECURE DISPOSAL	
6.1.8	Self-Evaluation Forms	Yes	Current year + 6 years	SECURE DISPOSAL	

8. Central Government and Local Authority

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

Appendix A – List of School Records and Data safely destroyed

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

Ref Number	File/Record Title	Description	Reference or Cataloguing Information	Number of Files Destroyed	Method of destruction	**Confirm** **(i) Safely destroyed** **(ii) In accordance with Data Retention Guidelines** **Tick (√)**
e.g.	*School Invoices*	*Copies of purchase invoices dated 2011/12*	*Folders marked "Purchase Invoices 2011/12" 1 to 3*	*3 Folders*	*Shredding*	√
1						
2						
3						
4						
5						
6						
7						
8						
9						
10						
11						
12						
13						
14						