





DATA PROTECTION POLICY, PRIVACY NOTICES and RETENTION POLICY

January 2024

Responsibility	Head Teacher
Date of next review by	31/12/2024

Signed: 
Chair of Governors

Date: 08.12.2023

Signed: 
Head Teacher

Date: 08.12.2023

Contents

1. Introduction	5
2. Scope and Responsibilities	5
3. Data Protection Legislation & Regulator.....	5
4. Our Data Protection Objectives	5
5. Our Data Protection Rules	6
6. Rights.....	8
7. Data Sharing.....	8
8. Non-UK data transfers	9
9. Data protection breaches	9
10. Related Policies	9
Appendix 1: Legal Conditions for Processing	10
1.1 Introduction	10
1.2 Our role and basis for processing	10
1.3 Special Category Data	11
1.4 Data Subjects' Rights.....	14
Appendix 2: Data Protection - Personal Data Breach Procedure	15
2.1 Introduction	15
2.2 Scope and Responsibilities.....	15
2.3 What is a Personal Data Breach?	15
2.4 Breach Response Plan	15
2.5 Data Breach Checklist	19
Appendix 3: Data Protection Impact Assessment Guidance and Template	20
3.1 Introduction	20
3.2 What is a Data Protection Impact Assessment (DPIA)?	20
3.3 When will a DPIA be appropriate?	20
3.4 The Benefits of a DPIA.....	21
3.5 Steps to be followed when considering a new project.....	21
3.6 Monitoring	21
Appendix 4: Subject Access Request (SAR) Procedure	22
4.1 Introduction	22
4.2 Scope and Responsibilities.....	22
4.3 Receiving a valid SAR.....	23
4.4 Responding to a SAR	24
4.5 Exemptions.....	24
4.6 SAR Request Form.....	25

Appendix 5: Freedom of Information requests under the Freedom of Information Act 2002	28
5.1 Introduction: what a publication scheme is and why it has been developed	28
5.2 Values.....	28
5.3 Categories of information published	28
5.4 Classes of Information Currently Published.....	29
5.5 How to request information	2
5.6 Advice & Assistance	2
5.7 Paying for information	3
5.8 Feedback and Complaints	4
Appendix 6: Privacy Notice: Workforce	5
6.1 Privacy Notice (How we use workforce information)	5
6.2 The categories of school workforce information that we process include	5
6.3 Why we collect and use workforce information.....	5
6.4 How we collect workforce information	6
6.5 How, where and for how long we store workforce information	7
6.6 Who we share workforce information with.....	7
6.7 Why we share school workforce information.....	7
6.8 Freedom of Information Act and Environmental Information Regulations 2004.....	8
6.9 Requesting access to your personal data	8
6.10 How Government uses your data	8
6.11 Contact us	9
Appendix 7: Privacy Notice: Pupils & Family.....	11
7.1 How we use pupil information.....	11
7.2 The types of information we process	11
7.3 Why we collect and use your information.....	11
7.4 How we collect pupil and family information	13
7.5 How, where and for how long we store pupil and family information	13
7.6 Who we share pupil information with.....	13
7.7 International Transfers	13
7.8 Freedom of Information Act and Environmental Regulations 2004.....	14
7.9 Why we regularly share pupil information	14
7.10 Requesting access to your personal data and other rights.....	15
7.11 How Government uses your information	15
7.12 Contact us	17
Appendix 8: Privacy Notice: School Governors.....	18
8.1 How we use governors' information	18
8.2 The categories of governors' information that we process include	18

8.3	Why we collect and use governors' information	18
8.4	How we collect governors' information	19
8.5	How, where and for how long we store governor's information	19
8.6	Who we share governors' information with	19
8.7	Why we share governors' information	20
8.8	Local Authority	20
8.9	Department for Education	20
8.10	Freedom of Information Act and Environmental Information Regulations 2004	20
8.11	Requesting access to your personal data	20
8.12	How Government uses your data	20
8.13	Sharing by the Department of Education	21
8.14	Contact us	21
Appendix 9: Retention and Deletions Policy		22
9.1	Introduction	22
9.2	Purpose	22
9.3	Disposal of Data	23
9.4	Transfer of records to Archives	23
9.5	Transfer of records to other Media	24
9.6	Transfer of records to other settings and 'last known school'	24
9.7	Responsibility and Monitoring	24
9.8	Retention Table	25

1. Introduction

- 1.1. This Policy lays out our approach to data protection. We recognise the importance of protecting the personal data we are entrusted with, and this policy sets out how we comply with relevant legislation.
- 1.2. If you have any queries about this Policy, please contact [our Data Protection Officer], whose details can be found in our Privacy Notices.

2. Scope and Responsibilities

- 2.1. This Policy applies to all staff, including temporary staff, consultants, governors, volunteers, and contractors, and anyone else working on our behalf.
- 2.2. All staff are responsible for reading and understanding this policy before carrying out tasks that involve handling personal data, and for following this policy, including reporting any suspected breaches of it to our Data Protection Officer.
- 2.3. All leaders are responsible for ensuring their team read and understand this policy before carrying out tasks that involve handling personal data, and that they follow this policy, including reporting any suspected breaches of it.
- 2.4. Our Data Protection Officer is responsible for advising us about our data protection obligations, dealing with breaches of this policy, including suspected breaches, identified risks, and monitoring compliance with this policy.

3. Data Protection Legislation & Regulator

- 3.1. Relevant legislation includes:
 - UK General Data Protection Regulation (GDPR).
 - Data Protection Act 2018 (DPA 2018), which enacts the GDPR in the UK and includes exemptions and further detail, as well as offences that individuals can be prosecuted for.
 - Privacy and Electronic Communications Regulations (PECR), which cover electronic direct marketing ("marketing" includes fundraising and promoting an organisation's aims, not just selling).
 - Freedom of Information Act 2000, which provides key definitions referred to in the other legislation.
 - Human Rights Act 1998.
 - Computer Misuse Act 1990, which covers unauthorised access to and use of, computers and computer materials.
- 3.2. In the UK, the Information Commissioner's Office (ICO) is the data protection regulator.
- 3.3. Breaches of data protection legislation can result in significant monetary penalties and damage to reputation, as well as the risk of real harm to people whose data is handled in an unfair or unlawful way. Individual members of staff may be prosecuted for committing offences under Sections 170 – 173 of the DPA 2018.
- 3.4. Individual member of staff may be prosecuted for committing offences under Sections 170-173 of the DPA 2018.

4. Our Data Protection Objectives

We are committed to making sure that:

- 4.1. Personal data is only processed in keeping with legal data protection principles. The principles include: data being processed lawfully, fairly and in a transparent manner; data being processed only for specific, explicit and valid purposes; data being adequate, relevant and accurate; data not being kept longer than is necessary; and data being kept secure.
- 4.2. We adopt a "Privacy by Design" and "Privacy by Default" approach.
- 4.3. We can demonstrate our accountability and compliance.
- 4.4. The people whose data we hold (Data Subjects) understand the ways and reasons why we process their data and can easily and fairly exercise their rights around their data.

- 4.5. We only share personal data when it is fair and lawful to do so. When we share data we do it in a safe and secure way.
- 4.6. Data is not transferred outside of the UK except where the country has made an 'adequacy decision' or the transfer is covered by 'appropriate safeguards', as defined in UK GDPR Article 46, or there is a specific situation as defined by UK GDPR Article 49.
- 4.7. All data breaches, including near misses, are managed properly and reported appropriately, so we can minimise any risks and improve practices in the future. This includes any breaches of the Data Protection Act (DPA 2018) where the individual responsible may be liable.

5. Our Data Protection Rules

5.1. We follow the legal Data Protection Principles:

- i. **Fair, lawful and transparent processing:** The reason for processing of personal data must meet one of the legal conditions listed in Article 6 of the UK GDPR. In addition, when "special categories" of personal data are being processed, the purpose must also meet one of the legal conditions listed in Article 9 of the GDPR. "Special categories" are information about a person's race or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health, genetic and biometric data, sexual life or sexual orientation.

Legal conditions: See Appendix 1 for an explanation of the Legal Conditions for Processing.

Other legislation: All processing must also comply with the other Data Protection Principles and any other relevant legislation, including the DPA 2018 and the Privacy and Electronic Communications Regulations (PECR) as appropriate. Any individual who obtains, discloses or retains data when they do not have permission to do so may be committing an offence under the DPA 2018 Section 170. All electronic "direct marketing" is subject to the PECR, which require us to obtain consent before sending direct marketing messages electronically by email or SMS ("marketing" includes fundraising and similar types of messages, not just selling).

Transparency: To be fair and transparent, our data processing, including how and why we process data, is explained in our Privacy Notices. We also explain how and why data will be processed at the point where we collect that data, as much as is reasonably possible, and especially if the processing is likely to be unexpected.

- ii. **Purpose limitations:** We only use the data we collect for the reasons we explained in our privacy notice. If we need to use it for another reason, we will inform our data subjects of the new reason for processing before we do it.
- iii. **Data limitations:** We minimise the amount of data that we collect and process, keeping it to only what is necessary for the reasons we are collecting it. We should never collect or keep any personal data "just in case".
- iv. **Data accuracy:** We will always try to make sure the data we hold is accurate and kept up to date as appropriate.
- v. **Data retention:** We will only keep personal data for as long as is necessary for the reasons for which we are processing it, and we will be transparent with our data retention schedules, which can be found in Appendix 9 of this document. Any individual who purposefully retains data that they do not have authority for may be committing an offence under the DPA 2018 Section 170.
- vi. **Data security & integrity:** We use both technical and organisational security measures to protect data from unauthorised or unlawful processing, or from accidental loss, destruction or damage. Security measures should be appropriate to the level of risk involved in the data and the processing.

Our measures include, but are not limited to, technical measures such as ICT systems security, ICT access controls, and encryption; and organisational measures such as business continuity plans, physical security of our premises and data, policies, procedures, training, audits and reviews.

Security is be considered at all times. This includes when data is being stored, used, transferred, or disposed of, whether the data is electronic or hard copy, and regardless of how and where the data is being accessed and stored, especially when data is sent or taken off site, or to another organisation.

Any individual who purposefully re-identifies pseudonymised information without permission may be committing an offence under the DPA 2018 Section 171.

Organisational measures include extensive staff training. All school staff are trained. This training may be delivered live and covers all aspects of Data Protection awareness. Key themes are explained, including lawful basis, consent, and breach and subject access request awareness. The training is based on 'lessons learned' from other schools, action taken by the ICO and incidents reported in the press. There is discussion, questions and debate. It includes an assessment which must be passed (75% is the pass score) in order for the attendee to obtain a certificate of completion.

This training is delivered in full every two years with refresher updates shared in between. A refresher 'inset' day pre-recorded presentation from the DPO is provided every September.

Top-up online training is also available.

- 5.2. Privacy by Design & Default: Wherever possible, we adopt a Privacy by Design & Default approach. When we are planning projects or new ways of working that involve processing of personal data, we will consider the data protection implications, and how to make sure we meet legal and good practice requirements, from the planning stages, and keep a record of the outcomes.

For particularly high-risk processing, whether from a new or adapted way of working with personal data, we will do this using formal Data Protection Impact Assessments (DPIAs), to document the risks, decision-making process and decisions made, including recommendations and actions.

High risk processing includes processing the data of children, especially if processing special categories of data about children.

A DPIA is always required before setting up CCTV systems or similar tracking technologies.

A DPIA may be carried out retroactively to decide if changes or new controls are needed for existing ways of working.

- 5.3. To demonstrate and support our compliance with data protection legislation, we keep records of the processing we carry out, we have appropriate policies and procedures in place, we train our staff in data protection, we have a Data Protection Officer in post, we carry out regular audits and reviews of our activities, and we record and investigate data security breaches.

Our records of processing include our contact details and information about why we are processing personal data, what type data we process, the categories of people we process data about, information about how long we hold the data, and general information about our security measures, as well as the types of external organisations the data is shared with, including any transfers outside of the UK, and the safeguards in place if data is transferred outside the UK.

6. Rights

We process personal data in line with the legal rights of data subjects', including their right to:

- Be informed about their data being processed, which links to the first Data Protection Principle of fair, lawful and transparent processing.
- Request access to their data that we hold (sometimes requests are known as [Data] Subject Access Requests, or DSARs or SARs).
- Ask for inaccurate data to be rectified.
- Ask for data to be erased (sometimes known as the "right to be forgotten"), in limited circumstances.
- Restrict processing of their data, in limited circumstances.
- Object to the processing, in some circumstances, including stopping their data being used for direct marketing.
- Data portability, which means to receive copies of some of their data in a format that can be easily used by another organisation or person.
- Not be subject to automated decision making or profiling if it has legal effects or similarly significant effects on the data subjects.
- Withdraw consent when we are relying on consent to process their data.
- Make a complaint to the ICO or seek to enforce their data-related rights through the courts.

We will respond to, and fulfil, all valid requests within one calendar month, unless it is necessary to extend the timescale, by up to two months in certain circumstances. Not all the rights are absolute rights, and we cannot always carry out the requested action in full, or at all. For example, the right to erasure may be limited in some circumstances because we are required to keep some records, and a number of exemptions in the DPA 2018 apply to SARs, meaning we can withhold some information in some situations.

In responding to requests we also explain to data subjects they have the right to make a complaint to the ICO or seek to enforce their rights through the courts.

Any individual who purposefully alters, defaces, blocks, erases, destroys or conceals information to prevent it being provided in a SAR to a data subject who has requested it, and has a right to receive it, may be committing an offence under the DPA 2018 Section 173.

7. Data Sharing

7.1. Data Processors: We rely on the services of a number of external organisations to support our work (both management and curriculum). These may include people, companies, systems and software that process personal data as part of the work they do on our behalf. These are our "data processors". When working with data processors, we will carry out appropriate due diligence checks to make sure that they can provide sufficient guarantees that they will comply with data protection legislation, including keeping data secure and cooperating with us to uphold data subjects' rights.

In accordance with UK GDPR Article 28, data processors will, amongst other things: only process personal data based on our instructions; keep the data secure; assist us to comply with our legal obligations and uphold data subjects' rights; delete or return the data at the end of the contract; and allow inspections and audits of their processing activities.

7.2. Third Parties: We will only share personal data with any other external organisations, including other data controllers such as agencies and other schools, when the sharing meets one or more appropriate legal condition, and is carried out in keeping with the data protection principles and while upholding

the rights of data subjects. Where necessary we will enter into Data Sharing Agreements (DSA), or similar agreements, to help facilitate the sharing of personal data. A DSA does not make the sharing lawful, it only provides a framework to work within, to help share data in an effective and safe way that respects people's data protection rights, when an appropriate and lawful reason to share the data has been identified.

8. Non-UK data transfers

Personal data will not be transferred outside the UK unless it is allowed by the conditions in Chapter V of the UK GDPR, including having appropriate safeguards in place or the transfer being necessary for a specific situation that allows it. A "non-UK transfer" includes storing data on cloud-based software and systems where the servers that are located outside the UK.

9. Data protection breaches

- 9.1. All breaches, or suspected breaches, of this policy will be reported immediately to the Data Protection Officer, and will be investigated appropriately, corrective and preventive action taken and recorded. This includes, but is not limited to, any personal data we handle being lost, or being shared, destroyed, changed or put beyond use when it should not be.
- 9.2. Specifically, breaches that are likely to result in a risk to any rights and freedoms of the data subjects affected, will be reported to the ICO within 72 hours of the school becoming aware of the breach.
- 9.3. If a breach is likely to cause a high risk to affected data subjects, we will also tell the data subjects, as soon as possible and without undue delay, to allow them to take any actions that might help to protect them and their data. We will also consider informing data subjects about a breach, even if we are not legally obliged to, if it is appropriate for other reasons, such as preserving open communication.
- 9.4. We will log all breaches, including those that are not reportable to the ICO.

10. Related Policies

Also see:

- Freedom of Information Publication Scheme

Appendix 1: Legal Conditions for Processing

1.1 Introduction

“Personal data” means any information where a living person is either identified or identifiable, from the information alone, or with other information. Personal data can include written information, pupil work, photographs, CCTV and film footage or voice recordings, in electronic format (which can include in social media, apps, databases or other electronic formats) or hard copy (including copies printed from electronic sources, and handwritten data when it is part of a filing system or intended to be filed).

“Special category data” is personal data that needs more protection because it is sensitive, and there are tighter controls around this type of data:

- personal data revealing racial or ethnic origin
- personal data revealing political opinions
- personal data revealing religious or philosophical beliefs
- personal data revealing trade union membership
- genetic data
- biometric data (where used for identification purposes)
- data concerning physical and mental health
- data concerning a person’s sex life
- data concerning a person’s sexual orientation

In addition, the DfE advises that Pupil Premium/FSM status is treated as Sensitive Data.

“Data Subjects” include our pupils, staff, contractors, parents, local authority contacts, and anyone else we might come into contact with.

“Data Controller” means the school, which alone or jointly with other Data Controllers, decides on why and how personal data is processed.

“Processing” means collecting, storing, using, sharing and disposing of data.

“Processors” are the external bodies who processes personal data on behalf of the controller.

1.2 Our role and basis for processing

The role of any school is to educate and safeguard children. These are statutory obligations and come from various Acts and statutory instruments that can be found here.

This means the overwhelming volume of our collection and processing data based on the legal condition listed in Article 6 (1) c of the UK GDPR that “processing is necessary for compliance with a legal obligation to which the controller is subject”. The relevant legal obligation depend on the specific data processing, but they include:

- Equality Act 2010
- Education (Governors’ Annual Reports) (England)(Amendment)Regulations 2002.
- Special Educational Needs and Disability Act 2001
- Health & Safety of Pupils on Educational Visits 1998
- Safeguarding Vulnerable Groups Act 2006
- Disability Discrimination Act(s)
- The Education Act 1944, 1996, 2002, 2011
- The Education & Adoption Act 2016
- The Education (Information About Individual Pupils) (England) Regulations 2013

- The Education and Skills Act 2008
- The Education (Pupil Registration) (England) Regulations 2006
- Statutory Guidance for Local Authorities in England to Identify Children Not Receiving Education – February 2007)
- The Education and Inspections Act 2006
- The Children Act 1989, 2004
- The Childcare Act 2006
- The Children & Families Act 2014
- Local Safeguarding Children Boards Regulations 2006 (SI 2006/90)
- The Localism Act 2011 Contract (traded services)

Processing personal data as part of some of our functions related to safeguarding children that do not directly linked to a statutory function above is based on Article 6 (1) e of the UK GDPR, that “processing is necessary for the performance of a task carried out in the public interest”.

When we wish to process data for any other reason, we will ask for consent as per Article 6 (1) a UK GDPR. Typically, this will be for areas of our work that includes the public celebration of our school and pupils’ work. Data Subjects, or their parent/guardian, retain the right to change their consent preferences at any time by notifying the Head Teacher.

1.3 Special Category Data

1.3.1 Introduction

As part of the School’s statutory and corporate functions, we process special category data and criminal offence data in accordance with the requirements of Article 9 and 10 of the General Data Protection Regulation (‘UK GDPR’) and Schedule 1 of the Data Protection Act 2018 (‘DPA 2018’).

Special category data is defined at Article 9 of the UK GDPR as personal data revealing:

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Genetic data
- Biometric data (where used for identification purposes)
- Data concerning physical or mental health, or
- Data concerning a natural person’s sex life or sexual orientation.

In addition, we treat Pupil Premium/Free School Meal Status as if it is Special Category data as recommended by the Department of Education as we recognise that data subjects expect this information to be particularly private.

Article 10 of the UK GDPR covers processing in relation to criminal convictions and offences. This includes personal data relating to the alleged commission of offences or proceedings for an offence committed or alleged to have been committed, including sentencing. This is collectively referred to as ‘criminal offence data’.

Some of the legal conditions for processing special category and criminal offence data require us to have an Appropriate Policy Document in place, setting out and explaining our procedures for securing compliance with the data protection principles and to have policies regarding the retention and erasure of such personal data.

This document satisfies the requirement of Schedule 1, Part 4 of the DPA 2018 and explains our processing of special category and criminal offence data.

In addition, it provides some further information about our processing of special category and criminal offence data where a policy document isn't a specific requirement. The information supplements our privacy notices.

1.3.2 Conditions for processing special category and criminal offence data

We process special categories of personal data under the following UK GDPR Articles:

- Article 9(2)(a) – the data subject has given explicit consent to the processing (when none of the other lawful basis apply.)

When we seek consent, we make sure that the consent is unambiguous and for one or more specified purposes, is given by an affirmative action and is recorded as the condition for processing. Examples of our processing that require consent include pupil and staff dietary requirements or consent for pupil pastoral support.

- Article 9(2)(b) – processing is necessary in the field of employment law. An example of this processing includes staff sickness absences.
- Article 9(2)(c) - processing is necessary to protect the vital interests of the data subject or of another natural person. An example of this would be using health information about a member of staff in a medical emergency.
- Article 9(2)(f) – for the establishment, exercise or defense of legal claims. Examples of our processing include processing relating to any employment tribunal or other litigation.
- Article 9(2)(g) - reasons of substantial public interest.

The school is a public authority. Our role includes the education and safeguarding of pupils. Our processing of personal data in this context is necessary for the carrying out of our role. An example of our processing includes processing pupil health information in order to ensure pupils receive appropriate education taking into account any additional health needs they have.

- Article 9(2)(h)- necessary to assess the working capacity of the employee. An example of this would be the provision of occupational health services to our employees.
- Article 9(2)(j) – for archiving purposes in the public interest. An example of this is that we maintain a school archive of photos and significant school events for historical purposes.

1.3.3 We process criminal offence data under Article 10 of the GDPR

Examples of our processing of criminal offence data include pre-employment checks and declarations by an employee in line with contractual obligations or being informed about a parent's criminal convictions where that may affect the safeguarding or wellbeing of relevant pupils. We also process CCTV data which may include footage of alleged criminal offence data. We process this under the Data Protection Act 2018 Schedule 1, Part 2 subsection 10 and Part 3 subsection 36 (substantial public interest in relation to any criminal category data).

1.3.4 Description of data processed

We process the special category data about our pupils that is necessary to fulfil our obligations as a school. This includes information about their health and wellbeing status and ethnicity. Further information about this processing can be found in our pupil and parent privacy notice.

We process the special category data about our employees, governors and volunteers that is necessary to fulfil our obligations as an employer. This includes information about their health and wellbeing, ethnicity, sexual orientation and their membership of any trade union. Further information about this processing can be found in our workforce privacy notice.

We also maintain a record of our processing activities in accordance with Article 30 of the GDPR.

We process Special Category data for the following purposes outlined in DPA 2018 Schedule 1:

- Employment law, social security law and social protection law
- Health or social care purposes
- Public health
- Archiving purposes in the public interest
- Statutory purposes
- Equality of opportunity or treatment
- Preventing or detecting unlawful acts
- Regulatory requirements relating to unlawful acts
- Counselling
- Safeguarding of children and of individuals at risk

We process criminal offence data for the following purposes in Schedule 1:

- Employment law, social security law and social protection law
- Statutory purposes
- Safeguarding of children and individuals at risk
- Where criminal offences are captured by CCTV footage

11.3.3 Procedures for ensuring compliance with the principles

Accountability principle

We have put in place appropriate technical and organisational measures to meet the requirements of accountability. These include:

- The appointment of a Data Protection Officer who reports directly to our highest management level.
- Taking a 'data protection by design and default' approach to our activities.
- Maintaining documentation of our data processing activities.
- Adopting and implementing data protection policies and ensuring we have appropriate written contracts in place with our data processors.
- Implementing appropriate security measures in relation to the personal data we process.
- Carrying out data protection impact assessments for our high risk processing.

We regularly review our accountability measures and update or amend them when required.

Principle (a): Lawfulness, Fairness and Transparency: Processing personal data must be lawful, fair and transparent. It is only lawful if and to the extent it is based on law and either the data subject has given their consent for the processing, or the processing meets at least one of the conditions in Schedule 1 of the DPA 2018.

We provide clear and transparent information about why we process personal data including our lawful basis for processing in our privacy notices, in our Data Protection Policy and this policy document.

Our processing for purposes of substantial public interest is necessary for the exercise of the functions conferred on the school by the legislation referred to in our main Data Protection Policy document.

Our processing for the purposes of employment relates to our obligations as an employer.

Principle (b): Purpose Limitation: We are authorised by law to process personal data for these purposes. We may process personal data collected for any one of these purposes (whether by us or another controller), for any of the other purposes here, providing the processing is necessary and proportionate to that purpose.

If we are sharing data with another controller, we will document that they are authorised by law to process the data for their purpose. We will not process personal data for purposes incompatible with the original purpose it was collected for.

Principle (c): Data Minimisation: We collect personal data necessary for the relevant purposes and ensure it is not excessive. The information we process is necessary for and proportionate to our purposes. Where personal data is provided to us or obtained by us, but is not relevant to our stated purposes, we will erase it.

Principle (d): Accuracy: Where we become aware that personal data is inaccurate or out of date, having regard to the purpose for which it is being processed, we will take every reasonable step to ensure that data is erased or rectified without delay. If we decide not to either erase or rectify it, for example because the lawful basis we rely on to process the data means these rights don't apply, we will document our decision.

Principle (e): Storage Limitation: All special category data processed by us for the purpose of employment or substantial public interest is, unless retained longer for archiving purposes, retained for the periods set out in our Retention Schedule. We determine the retention period for this data based on our legal obligations and the necessity of its retention for our business needs. Our retention schedule is reviewed regularly and updated when necessary.

Principle (f): integrity and confidentiality (security): Electronic information is processed within our secure network. Hard copy information is processed in line with our security procedures. Our electronic systems and physical storage have appropriate access controls applied. The systems we use to process personal data allow us to erase or update personal data at any point in time where appropriate.

1.4 Data Subjects' Rights

All of our data subjects have a number of rights – these are detailed in section 6 of this Policy above.

To exercise these rights or for further help and information about processing and our commitment to keeping data safe, please contact our Data Protection Officer:

Data Protection Officer	GDPR for Schools, Derbyshire County Council
DPO Email:	DPforschools@derbyshire.gov.uk
DPO Phone:	01629 532888
DPO Address:	Room 396, North Block, County Hall, Smedley Street, Matlock, Derbyshire, DE4 3AG

Appendix 2: Data Protection - Personal Data Breach Procedure

2.1 Introduction

2.1.1. We recognise that a breach of personal data could happen, despite our policies, procedures and measures in place to protect personal data, and we will respond to any breach as quickly as possible in order to minimise any risks or potential harm, to the school or to individuals.

2.1.2. This procedure supports our Data Protection Policy. It includes our guidelines for reacting to and handling an actual or suspected breach of personal data, as soon as we become aware of the incident, in line with the UK GDPR, the DPA 2018 and best practice.

2.2 Scope and Responsibilities

This policy applies to all instances when it is known or suspected that personal data that the school handles has been subject to a breach (see below for breach definition.)

All staff are responsible for reading, understanding and complying with this policy.

Our Data Protection Officer provides assistance and further guidance on data breaches. The Head Teacher (or delegated person) is responsible for taking the lead on the steps in this procedure once a breach, or suspected breach, has been reported internally, including reporting to the Data Protection Officer.

Any staff member becoming aware of a breach is responsible for immediately reporting it internally, **and** logging it on the GDPRiS portal, to ensure it can be handled appropriately.

2.3 What is a Personal Data Breach?

2.3.1 If personal data we handle is lost, destroyed, altered, disclosed, accessed or put beyond use when it should not be, this is a Personal Data Breach.

2.3.2 Where we *suspect* personal data has been subject to a breach, we will follow this procedure until we are sure that the personal data has or has not been breached.

2.3.3 A personal data breach can occur accidentally or intentionally, and can be caused by staff, by an external threat, or anyone else.

2.4 Breach Response Plan

All members of staff are responsible for taking all reasonable steps and cooperating with key staff in following this procedure when a breach is found or suspected.

The breach response plan has 8 steps, which are covered in detail below:

- Report the breach internally
- Record the breach (using the GDPRiS software where applicable)
- Assess the risk
- Contain and recover
- Notify the ICO of the breach (if applicable)
- Notify the affected Data Subjects of the breach (if applicable)
- Review
- Implement any necessary changes to prevent reoccurrence.

Use the Data Breach Checklist (see 2.6 below for all personal data breaches.

2.4.1 Report the breach internally (school staff):

As soon as you become aware of a breach, or possible breach, report it to the Head Teacher (or delegated person), who will lead on the breach response including informing the Data Protection Officer of the breach and keeping them updated on the investigation and actions.

The report should be made as soon as possible even if the breach is discovered outside of normal working hours.

2.4.2 Record the breach (school staff):

Log the breach (using the GDPRiS software where applicable). Include as many details as possible and attach documents or evidence if appropriate.

If full details are not available immediately, log what information *is* available, and add more detail as it becomes available.

2.4.3 Assess the risk (DPO):

Consider what harm could come from the breach, including who could be harmed, how they could be harmed, and how severe the harm could be, as well as how likely it is the harm will happen. This risk assessment, based on severity and likelihood, will depend on the types of information involved (how sensitive is it, what could be done with it?), how much information is involved, and how exposed the data is, as well as the individual circumstances of the data subjects (that the data is about).

As an example, if a laptop has been lost, if it is encrypted there is a very small chance of any data being accessed. But if hard copy documents have been lost or left unattended, they are much more likely to be accessed and read. As another example, if personal data is included in an email by accident, the data may be at more risk of being misused if the email has gone to a member of the public, rather than to another school.

As an example of the need to assess the data subjects' circumstances, accidentally disclosing an address might not pose a risk to most data subjects, but it could be very high risk for someone who is escaping domestic violence, or for the adoptive family of a child.

2.4.4 Contain and recover (School with DPO support):

Take reasonable actions to contain the risks, and/or recover the data, if possible. Containment and recovery actions could include, as appropriate:

- Attempting to find lost devices or paperwork.
- If devices have been stolen, report this to the police.
- If a breach is still occurring, for example, due to an ongoing IT issue, then IT should take appropriate steps to minimise the breach, such as closing down an IT system or server. In the event of a Cyber-attack, immediately report to the Action Fraud line on 0300 1232040.
- Warning staff and third parties, such as the Local Authority, to be aware of any "phishing" attempts that might be linked to personal data that has been accessed by criminals/unauthorised people.
- If data has been sent to, or shared with, someone it shouldn't have been, consider if you can contact them to recover the data. Bear in mind that "recall" doesn't usually work on externally sent emails.
- If bank details have been lost/stolen, consider contacting banks directly for advice on preventing fraudulent use.
- If the data breach includes any entry codes or IT system passwords, change these immediately and inform the relevant agencies and members of staff.

2.4.5 Notify the ICO of the breach (DPO):

Breaches that could cause a risk to people should be reported to the Information Commissioner's Office (the ICO – the UK's data protection regulator) and, in some cases, to the data subject(s) involved too.

Not all breaches will need to be reported. For example, if data is deleted in error it is technically a breach, but if the data is backed up and can be promptly reinstated, it does not represent a risk to data subjects.

If the DPO decides not to report a breach to the ICO and/or the data subjects involved, the decision and reasons will be recorded.

If it is likely the breach will result in a risk to people's rights and freedoms, and have an adverse effect on data subjects, causing them harm, it must be reported to the ICO.

Reports to the ICO must be made within 72 hours of us becoming aware of the breach. Information can be provided to the ICO in stages, giving them the details as and when we find out more, but the first contact must be within 72 hours.

The information to be provided to the ICO:

- A description of the personal data breach that has occurred including, where possible:
 - The types and approximate number of people whose data is involved.
 - The types and approximate number of personal data records involved.
- The likely consequences of the breach.
- The measures taken, or proposed to be taken, in response to the breach, including actions to mitigate any possible harm to data subjects.
- The name and contact detail of the Data Protection Officer, or any other contact details of people who can provide more information.

Guidance on how to report to the ICO is on their website: <https://ico.org.uk/for-organisations/report-a-breach/>

2.4.6 Notify the affected Data Subjects of the breach (DPO):

If the risk to data subjects is assessed as high, the breach must also be reported to everyone whose data is involved, to allow them to take any appropriate steps to protect themselves and so they are aware of anything that may happen. For example, if financial information has been lost or stolen, they can alert their bank for fraudulent activity, or if passwords have been lost or stolen they can change them on their accounts and any other accounts that they used the same password on.

We can choose to report to data subjects even if the risk is not high, if we consider it would be better for us to tell them about the breach for other reasons, such as supporting transparent relations and trust. In many circumstances it will be preferable for data subjects to hear about a breach from the School rather than from any other source.

2.4.7 Review

Once the immediate controls have been put in place, review how the breach happened, going right down to the root causes of the breach. Consider all possible impacts on the situation that may have caused, or contributed to, the breach. Identify what changes will help prevent any similar breaches in future.

The review stage also includes reviewing and evaluating the response to the breach. Consider how effective the response was, and if improvements could be made when handling any future breaches e.g.

- Did the person who first became aware of the breach know to report it internally?

- Did attempts to recover the data work?
- How could the breach have been handled better or quicker?

The breach, and outcomes of the review, should be reported to the next Full Governors meeting for discussion. If systemic or ongoing problems are identified, then an action plan will be drawn up to put these right. If the breach warrants a disciplinary investigation, the manager leading the investigation may liaise with Human Resources or Internal Audit for advice and guidance.

2.4.8 Implement any necessary changes to prevent reoccurrence.

Depending on what the review indicates about how the breach occurred, actions should be taken to reduce the risk of something similar happening, including amongst other things, improved IT security, new or improved written procedures, refresher training, improved supervision, changes to processes, communications to remind colleagues about risks, etc.

2.5 Data Breach Checklist

Action	Taken? Give dates, initials and links to docs where appropriate
Date and time of discovery	
Date and time of occurrence	
What happened	
Immediate steps taken to contain the breach, e.g. changing passwords, shutting computers down, halting network traffic, restore data from backups	
Acknowledge breach by thanking informant for information – log it here	
Inform DPO 01629 532888	
Assess Risk:	[Consider how many people are affected, what type of data is involved, how could people be harmed, and how likely are they to be harmed?]
Necessary to inform ICO? 0303 1231113	
Date and time reported to ICO	
Necessary to inform data subjects?	
Data subjects informed?	
Police informed?	
Any other third parties informed	[Consider banks, suppliers, anyone else who needs to know about the breach.]
Review:	[Consider what was in place that should have prevented the breach, and why it failed, how could further breaches be prevented, how have we helped the people effected? Should we improve security, procedures, training, etc.?]
Steps taken to avoid reoccurrence	
Concluding letter	
SLT / Governors de brief	
Report completed by	

Appendix 3: Data Protection Impact Assessment Guidance and Template

3.1 Introduction

A Data Protection Impact Assessment (DPIA) is a tool to help us identify how to comply with our data protection obligations and protect individuals' rights.

An effective DPIA carried out in the earliest planning stages of a project or change to policy will allow us to identify and fix problems at an early on, reducing the associated costs, risks and damage to reputation which might otherwise occur.

This guidance explains the principles which form the basis for a DPIA, sets out the basic steps to carry out during the assessment process and includes a template which can be adapted as needed to fit the project.

DPIAs should be drawn up with the assistance of the DPO, who will have the expertise needed to fully consider the issues, but the responsibility for ensuring the DPIA is undertaken lies with the staff member responsible for the project or policy.

3.2 What is a Data Protection Impact Assessment (DPIA)?

A DPIA is a process which helps an organisation to identify and reduce the privacy risks of any project which involves personal data. To be effective a DPIA should be used throughout the development and implementation of the Academy's project.

A DPIA will enable the Academy to systematically and thoroughly analyse how a particular project or system will affect the privacy of the individuals involved, as well as provide evidence of investigation into the suitability of any third parties who will be given access to data in the project.

3.3 When will a DPIA be appropriate?

DPIAs should be considered for all new projects, at the earliest stages to allow greater scope for influencing how the project will be implemented. A DPIA can also be useful when planning changes to an existing system.

The school must carry out a DPIA for processing that is likely to result in a "high risk to individuals" (Article 35(1) UK GDPR). When considering if the processing is likely to result in high risk, the Academy and the DPO should consider the relevant ICO Guidance.

<https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/>

These list types of data processing operations that are likely to result in high risk. The two most relevant to schools relate to processing of vulnerable data subjects (children) and the processing of Sensitive Data or data of a highly personal nature. Because so many activities in schools include the processing of children's data including Sensitive Data, it is likely that most projects in schools will require a DPIA to be carried out.

Conducting a DPIA does not have to be complex or time consuming but there must be a level of rigour in proportion to the potential privacy risks.

3.4 The Benefits of a DPIA

Consistent use of DPIAs will increase the awareness of privacy and data protection issues within the Academy and ensure that all relevant staff involved in designing projects think about privacy at its earliest stages.

Examples of where a DPIA would be appropriate

- Purchasing/implementing a new IT system for storing and accessing personal data.
- A data sharing initiative where two or more schools seek to pool or link sets of personal data.
- A proposal to identify people in a particular group or demographic and take action in relation to the group.
- Using existing data for a new and unexpected or more intrusive purpose.
- A new database which consolidates information held by separate parts of the school.
- Legislation, policy or strategies which will impact on privacy through the collection or use of information, or through surveillance or other monitoring.
- Purchasing/implementing cloud hosted applications.
- The collection of new data on an existing system.
- Setting up a CCTV system.

3.5 Steps to be followed when considering a new project

A DPIA should be undertaken before a project is underway, in the same way that schools consider the cost impact of a project before making a commitment to spend any money. Consultation should be made with the DPO, and consideration should be given to consulting with affected data subjects as a first step. The DPIA process should be a collaborative task between the Data Protection Lead (Director of Operations) and staff who will be using the system/managing the project under consideration.

3.6 Monitoring

The completed DPIA should be checked and approved by the DPO and then submitted to the Governing Body for final review and approval. The Governing Body will monitor implementation of actions identified in DPIAs.

Further details and templates for completing a DPIA are available on the GDPRiS portal

Appendix 4: Subject Access Request (SAR) Procedure

4.1 Introduction

- 4.1.1 We process personal data in line with all of the legal rights of data subjects', including their right to:
- Be informed about their data being processed, which links to the first DP Principle of fair, lawful and transparent processing.
 - Request access to their data that we hold.
 - Ask for inaccurate data to be rectified.
 - Ask for data to be erased (sometimes known as the "right to be forgotten").
 - Restrict processing of their data, in limited circumstances.
 - Object to the processing, in some circumstances, including stopping their data being used for direct marketing.
 - Data portability, which means to receive copies of some of their data in a format that can be easily used by another organisation or person.
 - Not be subject to automated decision making or profiling if it has legal effects or similarly significant effects on the data subjects.
 - Withdraw consent when we are relying on consent to process their data.
 - Make a complaint to the ICO or seek to enforce their rights through the courts.
- 4.1.2 This procedure supports our Data Protection Policy, and explains how we respond to requests from, or on behalf of, individuals for access to the data we hold that is about the individual. This is known as the right to access and is a legal right under the UK GDPR and the DPA 2018. Requests are known as [Data] Subject Access Requests, or DSARs or SARs.
- 4.1.3 In addition, pupils, or parents on their behalf, have the right to access the pupil's curricular and educational records relating to the pupil, under the Education (Pupil Information) (England) Regulations 2005 (EPIR 2005).
- 4.1.4 For any queries about how to exercise any of the rights above, contact our Data Protection Officer.

4.2 Scope and Responsibilities

The right to access applies to all pupils, parents, staff and anyone else that we hold personal data about. In some circumstances, for example with pupils, a parent or other person with authority may make the Subject Access Request on their behalf.

All staff are responsible for reading and understanding this procedure if they may receive a SAR on behalf of the school, as SARs can be made through any member of staff, although responses should be centrally coordinated.

Our Data Protection Officer (DPO) provides assistance and further guidance on responding to SARs and coordinates all responses.

Any individual who purposefully alters, defaces, blocks, erases, destroys or conceals information to prevent it being provided to a data subject who has requested it, and has a right to receive it, may be committing an offence.

4.3 Receiving a valid SAR

Format: An SAR does not need to be in writing, it can be in any format, including a letter, email, text message, over social media, over the telephone, or face to face, and can be made to any representative of the school.

However, in order to process the request as efficiently as possible, and to help us comply with statutory timeframes, we ask that the form contained in Section 4.6 below is completed.

Content: An SAR does not need to refer to data protection legislation or be described as a subject to be a valid SAR. Any request for access to personal information from, or on behalf of, a data subject, should be treated as a SAR.

Identity & Authority: We must verify the identity of the person making the SAR, and if the SAR is being made on behalf of someone else, we must confirm they have authority to act on their behalf in exercising their rights. Checking identity should not be used as a delaying tactic, and how to verify identity will depend on who is making the SAR, and how well they are known to the person handling the request. For example, a staff member will not usually be required to confirm their identity, but a request from a former staff member, or on behalf of someone else, would need to be verified using proof of identity, signature and address.

A parent/person with parental responsibility does not automatically have the right to make a SAR on behalf of their child.

A child may exercise these rights on their own behalf if we believe they are competent to do so. Assessing competence is based on the age, maturity and level of understanding of the child. Each situation will be decided in collaboration with the professionals working with the child, but 12 years is regarded as a starting point. A child should not be considered competent if it is evident that he or she is acting against their own best interests or under pressure from a parent or other person with authority.

Where a SAR is received from a parent of a competent child, consent to process the request and release all/part of the information will be sought from the child.

No charge: In most cases, an SAR will be responded to free of charge. In limited circumstances, where a request is manifestly unfounded or excessive an appropriate charge can be made. Requests made under EPIR 2005 may be charged for. A proposed charge should be agreed with the DPO.

Refusing to fulfil a SAR: In limited circumstances, the request or elements of it, may be refused under the exemptions in the DPA 2018, for example:

- If the requestor cannot confirm their identity or authority to make the request on behalf of another person, the request will be refused until confirmation is provided.
- Where a request is manifestly unfounded or manifestly excessive.
- Information relating to education data, social work or health data if might cause serious harm to the physical or mental health of the data subject or another individual (this applies even when a competent child has consented to their parent receiving their data).

Elements of data held may be withheld or redacted, include:

- Information that would reveal that a child is at risk of abuse, where disclosure of that information would not be in the child's best interests (this applies even when a competent child has consented to their parent receiving their data).
- Information contained in adoption and parental order records.
- Certain information given to a court in proceedings concerning a child.

4.4 Responding to a SAR

Timescales: SARs must be responded to as soon as possible, and within one month at the latest. In the case of complex or multiple requests an extension of up to an extra two months can be applied, but the requestor must be informed of the extension within the first month from the SAR. The calculation of time will commence once the SAR is determined as valid. An acknowledgement should be sent to the requestor as soon as possible to inform them that the SAR has been received, the start date, and that it is being processed.

For SARs, school holidays, bank holidays and weekends are all included within the month. For example, a valid SAR received on 20th July should be fulfilled by 20th August despite the school closure.

Format: The DPO will decide with the requestor, the most appropriate and preferred method of providing information.

Content: The 'right to access' allows the requestor to receive information held about them, as a Data Subject. The requestor will not necessarily receive every version of information if it is held in different ways or duplicated. Access is to the data, not the particular documents.

Third party data: Where the person's data is combined with another person's data, which does or could identify that other person (third party), that data may be redacted, or withheld if redaction would not fully prevent the other person being identified. Data can be disclosed that identifies the third party if, that person has given their consent to disclose it, or it is judged to be reasonable to disclose the information without that person's consent. Deciding if it is reasonable should take into account things such as the type of information, any duty of confidentiality owed, the role of the other person, whether the person is capable of giving consent, and whether they have expressly refused consent.

4.5 Exemptions

Exemptions apply under the DPA 2018, allowing us to withhold data from an SAR in some further circumstances, including amongst others: where legal professional privilege applies, where management forecasts or negotiations could be prejudiced by disclosing the data, confidential references, and where exam results are requested but they are not yet due to be published.

The application of exemptions should be approved by the DPO, but **if in doubt do not disclose information**, as it can always be disclosed at a later date.

Response: When sending the relevant data to the requestor, the information should be clear, so any codes or jargon used should be explained in the SAR response. In responding to requests we also explain to data subjects they have the right to make a complaint to the ICO or seek to enforce their rights through the courts.

Data subjects also have a right to receive, in response to their SAR, the following information, which is contained within our Privacy Notice (a copy of which will accompany the release):

- The purposes of our processing.
- The categories of personal data concerned.
- The recipients or categories of recipient we disclose the personal data to.
- Retention periods for storing the personal data or, where this is not possible, our criteria for determining how long you will store it.
- The existence of their right to request rectification, erasure or restriction or to object to such processing.

- Information about the source of the data, where it was not obtained directly from the individual.
- The existence of any automated decision-making (including profiling); and
- The safeguards we provide if we transfer their personal data to a third country or international organisation.

Monitoring: The receipt of SARs will be logged and coordinated centrally, using GDPRiS where appropriate, to ensure timescales are being met and SARs are being handled appropriately.

4.6 SAR Request Form

Section 1

About you or person you are making this request on behalf of; this information will help us to identify the personal data that we may hold about you.

Title: Mr/Mrs/Miss/Ms/Dr/Rev etc.	
Surname/Family Name:	
First Name(s):	
Maiden/Former Name(s): (If applicable)	
Date of Birth: (dd/mm/yyyy)	
Home Address: (including postcode)	
Alternative address for correspondence: (if different to above)	
Contact telephone number:	
Contact e mail address:	
Name of person making request (if different to above). This is the address to which all replies will be sent unless specified otherwise.	
Surname/Family Name:	
First Name(s):	
Relationship to data subject:	
Address: (including postcode)	
Contact telephone number:	
Contact e mail address:	

Section 2: About your request

What records that you believe we hold would you like access to:	
Have you made a request for this information before? (Yes/No)	
If Yes, could you please provide date of request? (dd/mm/yyyy)	
Where do you want to view your information? For example in person, or be sent a paper copy to your home or alternative address or be sent a copy in a specific electronic format to an e mail address (if this is your preferred option we would encrypt the file to keep it secure).	
Do you need any other help with this request? (Please specify below)	

Section 3: Proof of identity

Establishing Proof of Identity

If we have a verified current address for you on our systems we will contact you at that address and ask you to confirm that the request has come from yourself. If this is not possible, we will ask for documentary evidence to verify you are who you say you are.

To help establish your identity we may ask you to provide at least two different documents which, between them, provide sufficient information to prove your name, date of birth, current address and signature. For example, a combination of driving licence, birth/adoption certificate, passport and any other official documents e.g. utility bills, which show those details.

If you are making this request on behalf of someone else you must provide evidence you have the right to do so, e.g. letter of consent, birth certificate evidencing you have parental responsibility for a child or any other relevant legal documentation, unless you have supplied this information to us already for other purposes.

On receipt of completed form we will contact you to arrange verification of these documents.

Please note that it may be necessary to seek further information or proof of identity (of data subject or requestor) before the request can be processed. If this is the case, then the statutory one month day limit

will start from the date all necessary information and proof is received. Every effort will be made to provide you with your information as soon as possible after receipt of your application, however in some cases we may need longer than a month to respond to your request if any complex issues are involved.

Section 4: Declaration: To be signed by the Requestor

The information, which I have supplied in this application, is correct, and I am the person to whom it relates/I have the right to make this request on their behalf (delete as appropriate).

Name:	
Signature:	
Date	

Warning: A person who impersonates another or attempts to impersonate another may be guilty of an offence. It is similarly an offence to coerce consent from a Data Subject or interested third party.

Should any advice or guidance be required in completing this application, please contact our Data Protection Officer (see below).

General advice on the UK GDPR and Data Protection Act 2018 can be obtained from The Information Commissioners' Office, contact details are below.

The information on this form will only be used to support you in exercising your rights under the Data Protection Act 2018 and will be destroyed, in line with our retention policy, after a decision on your request has been made. For further information on how Derbyshire County Council may use your personal information visit: www.derbyshire.gov.uk/privacynotices

Please return this form once completed to:

FAO Data Protection Officer: The Aspire Academy, Bridgwater Road, Worcester. WR4 9DQ

Mark your envelope "Subject Access Request - Confidential".

Data Protection Officer Education Data Hub (GDPR for Schools), Derbyshire County Council

DPO Email: DPforschools@derbyshire.gov.uk

DPO Phone: 01629 532888

DPO Address: Room 396, North Block, County Hall, Smedley Street, Matlock, Derbyshire, DE4 3AG

If however you are dissatisfied with our response, you can of course contact the ICO quoting our ICO registration number ZA063714 and stating that the Data Controller is **The Aspire Free School Academy Trust**.

Information Commissioners' Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

Tel: 0303 123 1113 (local rate) or 01625 545 745 if you prefer to use a national rate number

Fax: 01625 524 510. Website: <https://ico.org.uk/concerns/>

Appendix 5: Freedom of Information requests under the Freedom of Information Act 2002

5.1 Introduction: what a publication scheme is and why it has been developed

One of the aims of the Freedom of Information Act 2000 (FOIA) is that public authorities, should be clear and proactive about the information they will make public.

To do this we must produce a publication scheme, setting out:

- The classes of information which we publish or intend to publish.
- The manner in which the information will be published.
- Whether the information is available free of charge or on payment.

The scheme (in 5.6 below) covers information already published and information which is to be published in the future.

Some information which we hold may not be made public, for example personal information.

This publication scheme conforms to the model scheme for schools approved by the Information Commissioner.

5.2 Values

Our Ethos at the Aspire Academy is committed to providing:

A safe, containing, caring, good humoured and well-disciplined school where strong nurturing relationships and an understanding of childhood trauma and attachment issues are at the heart of everything.

A world class Alternative Provision in which we present:

- An environment where all pupils can thrive, grow, heal and achieve through a relentlessly reasonable approach to personal development.
- Opportunities for pupils to build their social capital, resilience, self-esteem and a portfolio of recognised qualifications in order that they may make a positive next-step.
- All pupils with the opportunities to achieve a positive destination when they leave the Academy.

In addition to our obligations under the FOIA, we seek to be as transparent as possible with our community and stakeholders. This appendix outlines how we will respond to requests.

5.3 Categories of information published

This publication scheme guides you to information which we currently publish (or have recently published) or which we will publish in the future. This is split into categories of information known as 'classes'. These are contained in section 5.4 below.

The classes of information that we undertake to make available are organised into 3 broad topic areas:

1. *School Prospectus* – information published in the school prospectus/website.
2. *Governors' Documents* – information published in governing body documents.
3. *School Policies [including Pupils & Curriculum]* and other information related to the school - information about policies that relate to pupils and the school curriculum and the school in general.

5.4 Classes of Information Currently Published

5.4.1 School Prospectus/website – this section sets out information published in the school prospectus/website.

The statutory contents of the school prospectus/website are as follows, (other items may be included in the prospectus at the school's discretion):

- The name, address and telephone number of the school, and the type of school
- The name of the Head Teacher
- Safeguarding
- A statement of the school's ethos and values
- Governance Information
- School Referral Forms
- Curriculum offer
- Careers
- Remote Learning
- Parent Information

5.4.2 Governing Body Documents

This section sets out information published in governing body documents.

- Makeup of the Governing Body
- Governor meeting attendance
- Funding Agreement
- Financial Statements

5.4.3 School Policies & Information [including pupils & curriculum] - This section sets out details of policies and information that can be found on the school website. Some information might be confidential or otherwise exempt from the publication by law – we cannot therefore publish this:

- | | |
|---|--|
| • Accessibility | • Equality Objective and Action Plan |
| • Admissions | • SENDIASS Exclusions Advice |
| • Anti-bullying | • Finance Policy |
| • Assessment | • First Aid, Administering Medication & Supporting Pupils with Medical Needs |
| • Attendance | • Freedom of Information Publication Scheme |
| • Behaviour | • Grievance and Harassment Procedure |
| • Capability | • Health & Safety |
| • Careers Strategy | • Home School Agreement |
| • CCTV | • Lettings |
| • Charging & Remissions | • Looked After Children |
| • Child on Child Abuse | • On-line Safety (including ICT Acceptable Use) |
| • Complaints Procedure | • Pay Policy |
| • CPD | • Pecuniary Interests |
| • Curriculum | • Preventing Extremism & Radicalisation |
| • Data Protection, Privacy and Retention Policy | • Pupil Premium |
| • Educational Visits | |
| • Equal Opportunity (including Race, Equality and Cultural Diversity) | |

- Quality Assurance for Delivery of Qualifications
- Relationships & Sex (RSE)
- Remote Learning
- Reserves
- Safeguarding Children
- SEND
- Staff Induction
- Staff Malpractice
- Suspension and Permanent Exclusion
- Teaching & learning
- Visitors in School
- Whistleblowing
- Work Experience

5.4.5 Other information related to the school

- Published report of the last inspection of the school and the summary of the report
- School session times and term dates
- School Calendar (including INSET days)

5.5 How to request information

Where information is not published on our website, you may make a request by contacting the school in writing, by email or letter.

To help us process your request quickly, please clearly mark any correspondence **“FREEDOM OF INFORMATION REQUEST”**.

We will, no later than 20 working days from receipt of the request:

- Confirm or deny whether we hold information of the description specified in the request
- Provide the documentation, if we hold the requested information.

Except where:

- We reasonable require further information to meet a freedom of information request, have informed the requestor of this requirement, but have not been supplied with that further information.
- The information is no longer readily available as it is contained in files that have been placed in archive storage or is difficult to access for similar reasons.
- A request for information is exempt under section 2 of the Freedom of Information Act 2000.
- The cost of providing the information exceeds the appropriate limit.
- The request is vexatious.
- The request is a repeated request from the same person made within 60 consecutive working days of the initial one.
- A fee notice was not honoured.

Where information is, or is thought to be, exempt, we will, within 20 working days, give notice to the requestor which:

- States the fact, and
- Specifies the exemption in question.

5.5.1 Format

The information provided will be in the format requested, where possible. Where it is not possible to provide the information in the requested format, we will assist the requestor by discussing alternative formats in which it can be provided.

The information provided will also be in the language in which it is held, or another language that is legally required. Translations and alternative formats required under relevant disability and discrimination regulations will be provided where necessary.

5.5.2 The appropriate limit

The school will not comply with any freedom of information request that exceeds the statutorily imposed appropriate limit of £450.

In determining whether the cost of complying with a freedom of information request is within the appropriate limit, we will take account only of the costs we reasonably expect to incur in relation to:

- Determining whether we hold the information.
- Locating the information, or a document which may contain the information.
- Retrieving the information, or a document which may contain the information.
- Extracting the information from a document containing it.
- Costs related to the time are to be estimated at a rate of £25 per person per hour.

Where multiple requests for information are made to the school within 60 consecutive working days of each other, either by a single person or by different persons who appear to be acting in concert, the estimated cost of complying with any of the requests is to be taken to be the total costs to the school of complying with all of them.

5.6 Advice & Assistance

The school has a duty to provide advice and assistance and will do so in the following circumstances.

- If an individual requests to know what types of information the school holds and the format in which it is available, as well as information on the fees regulations and charging procedures.
- If a request has been made, but the school is unable to regard it as a valid request due to insufficient information, leading to an inability to identify and locate the information.
- If a request has been refused, e.g. due to an excessive cost, and it is necessary for the school to assist the individual who has submitted the request.

The school will provide assistance for each individual on a case-by-case basis; examples of how the school will provide assistance include the following: This list is not exhaustive, and we may decide to take additional assistance measures that are appropriate to the case.

- Informing a requestor of their rights under the Freedom of Information Act 2000
- Assisting an individual in the focus of their request, e.g. by advising of the types of information available within the requested category
- Advising a requestor if information is available elsewhere and how to access this information
- Keeping a requestor informed on the progress of their request

In order to provide assistance as outlined above, the school will engage in the following good practice procedures:

- Make early contact and keep the requestor informed of the process of their request.
- Accurately record and document all correspondence concerning the clarification and handling of any request.
Give consideration to the most appropriate means of contacting the requestor, taking into account their individual circumstances.
- Remain prepared to assist a requestor who has had their request denied due to an exemption.

The school will give particular consideration to what level of assistance is required for a requestor who has difficulty submitting a written request.

In circumstances where an requestor has difficulty submitting a written request, the school will:

- Make a note of the application over the telephone and then send the note to the requestor to confirm and return – the statutory time limit for a reply would begin here.
- Direct the individual to a different agency that may be able to assist with framing their request.

This list is not exhaustive and the school may decide to take additional assistance measures that are appropriate to the case.

Where a requestor's request has been refused either because the information is accessible by other means, or the information is intended for future publication or research, the school, as a matter of good practice, will provide advice and assistance.

The school will advise the requestor how and where information can be obtained, if it is accessible by other means.

Where there is an intention to publish the information in the future, the school will advise the requestor of when this publication is expected.

If the request is not clear, the school will ask for more detail from the requestor in order to identify and locate the relevant information, before providing further advice and assistance.

If the school is able to clearly identify the elements of a request, it will respond following usual procedures and will provide advice and assistance for the remainder of the request.

If any additional clarification is needed for the remainder of a request, the school will ensure there is no delay in asking for further information.

If a requestor decides not to follow the school's advice and assistance and fails to provide clarification, the school is under no obligation to contact the requestor again.

If the school is under any doubt that the requestor did not receive the advice and assistance, the school will re-issue it.

The school is not required to provide assistance where a requestor's request is vexatious or repeated, as defined under section 14 of the Freedom of Information Act 2000.

The school is also not required to provide information where the cost of complying with a request exceeds the limit outlined in the Freedom of Information Act 2000. In such cases, the school will consider whether any information can be provided free of charge if the requestor refuses to pay the fee.

A record will be kept by the School of all the advice and assistance provided.

5.7 Paying for information

Information published on our website is free, although you may incur costs from your Internet service provider. If you don't have Internet access, you can access our website using a local library or an Internet café.

Single copies of information covered by this publication are provided free unless stated otherwise in section 6. If however your request means that we have to do a lot of photocopying or printing, the following charges will apply:

- 5p per single side of A4,
- 10p per single side of A3.
- plus any postal charge at the current rate applied by Royal Mail.

For a priced item such as some printed publications or videos we will let you know the cost before fulfilling your request. Where there is a charge this will be indicated on application on an individual basis.

5.8 Feedback and Complaints

If you want to make any comments about this publication scheme or if you require further assistance or wish to make a complaint please contact the School Office, Headteacher or School Data Protection Officer:

Data Protection Officer	Education Data Hub (GDPR for Schools), Derbyshire County Council
DPO Email:	DPforschools@derbyshire.gov.uk
DPO Phone:	01629 532888
DPO Address:	County Hall, Smedley Street, Matlock, Derbyshire, DE4 3AG

If however you are dissatisfied with our response, you can of course contact the ICO quoting our ICO registration number **ZA063714** and stating that the Data Controller is **The Aspire Free School Academy Trust**.

Information Commissioners Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

Tel: 0303 123 1113 (local rate) or 01625 545 745 if you prefer to use a national rate number

Fax: 01625 524 510

Website: <https://ico.org.uk/concerns/>

Appendix 6: Privacy Notice: Workforce

6.1 Privacy Notice (How we use workforce information)

We collect, hold, use and share information about our workforce. This is known as “personal data” and you have rights around that data, including knowing how and why we are processing the data. “Processing” data means everything from collecting, to storing, using, sharing and disposing of it. The School workforce includes all those employed to teach, or otherwise engaged to work, either on a paid, contracted or voluntary basis, at the school.

For the purposes of Data Protection legislation The Aspire Free School Academy Trust is a data controller and is registered as such with the Information Commissioner’s Office.

Our Data Protection Officer is **GDPR for Schools, Derbyshire County Council** (see ‘Contact us’ below).

6.2 The categories of school workforce information that we process include

- Personal information (such as name, address, employee or teacher number, National Insurance number).
- Characteristics information (such as gender, age, ethnic group)*.
- Contract information (such as start date, hours worked, post, roles and salary information).
- Work absence information (such as number of absences and reasons) and relevant medical information.
- Qualifications (and, where relevant, subjects taught).
- Photographic and CCTV records*.
- Information about medical or health conditions, including whether you have a disability for which the school needs to make reasonable adjustments
- Date of birth, marital status and gender
- Details of trade union membership if you pay your subscriptions through payroll*.
- Equalities monitoring information, including information about your ethnic origin, sexual orientation, health and religion or belief*.
- Next of kin and emergency contact details
- Salary, annual leave, pension and benefits information
- Bank account details, payroll records, national insurance number and tax status information
- Recruitment information, including right to work documentation, references and other information included in an application form and/or CV, or covering letter or as part of the application process
- Performance information
- Information relating to grievance and/or disciplinary procedures
- Copy of driving licence (or equivalent) and motor insurance certification

We may also collect, use, store and share (when appropriate) information about criminal convictions, offences and prohibitions. This information may have come from other organisations including former employers, Teacher Regulation Agency, social services and the Disclosure & Barring Service.

6.3 Why we collect and use workforce information

We use the workforce to:

- a) Enable the development of a comprehensive picture of the workforce and how it is deployed.
- b) Inform the development of recruitment and retention policies.
- c) Enable individuals to be paid.

- d) Facilitate safer recruitment (e.g. by carrying out criminal records checks and requesting references).
- e) Support effective performance management
- f) Allow better financial modelling and planning.
- g) Support the management of absence.
- h) Photographic images for identification purposes (safeguarding), and celebration purposes (to record work, classes and school event).
- i) To meet our statutory duties
- j) For site safety and security
- k) To protect public monies against fraud
- l) To detect and prevent crime and combat fraud.
- m) To streamline systems.

Under the UK General Data Protection Regulation (UK GDPR), the legal basis for processing your personal data information include:

- Article 6(a): Your consent (for any processing which does not fall into the other bases explained below).
- Article 6(b): Contract (your contract of employment).
- Article 6(c): Compliance and with our legal obligations.

In particular, but not exclusively, section 5 of the Education (Supply of Information about the School Workforce) (England) Regulations 2007 and amendments.

- Article 6(e): Carrying out tasks in the Public Interest.
- Article 6(f): For legitimate Interests.

The ways we collect and use sensitive workforce information are lawful based on: your explicit consent; for compliance with certain legal obligations, or for exercising certain legal rights; for protecting a person's vital interests in an emergency; for health and public health reasons; or for carrying out tasks that are in the substantial public interest including for safeguarding purposes.

Please refer to the Data Protection Policy for full details of these lawful bases for processing this data. Types of data that are special category are indicated above by *.

6.3.1 Marketing purposes

Where you have given us consent to do so, we may send you marketing information by e-mail or text promoting school events, campaigns, charitable causes or services that may be of interest to you.

You can withdraw consent or 'opt out' of receiving these e-mails and/or texts at any time by contacting us (see 'Contact us' below).

6.3.2 Automated decision making and profiling

We do not currently process any personal data through automated decision making or profiling. If this changes in the future, we will amend any relevant privacy notices in order to explain the processing to you, including your right to object to it.

6.4 How we collect workforce information

We collect this information in a variety of ways. For example, data is collected through application forms, obtained from your passport or other identity documents such as your driving licence, from forms completed by you at the start of or during employment (such as pension benefit nomination forms), from correspondence with you, or through interviews, meetings or other assessments, self-certification

forms [medical], Fit Notes, images provided by individuals or taken using school photographic equipment, local authorities, previous employers, NHS, the Police, the Disclosure and Barring Service and the Department for Education [DfE].

Workforce data is essential for the School's/Local authority's operational use. Whilst the majority of personal information you provide to us is mandatory, some of it is requested on a voluntary basis. We will inform you at the point of collection, whether you are required to provide certain information to us and your rights in relation to this.

6.5 How, where and for how long we store workforce information

We store workforce information securely on the School's IT network, backed up through Redstor. Secure storage is provided for paper based records.

We only keep the information for the length of time we need it for, as shown in our data retention schedule. For more information on our data retention schedule please refer to Appendix 9 of this document, this can also be accessed within the staff e-handbook. We dispose of personal information securely when we no longer need it.

6.6 Who we share workforce information with

We routinely share this information with:

- Our Local Authority (particularly in relation functions related to HR Employee Services and Criminal Records checks). Worcestershire County Council.
- Our Governing Body
- The Department for Education (DfE)
- HMRC
- The Disclosure and Barring Service
- Employers where references are requested
- Police
- External systems/third parties used by the school to carry out day to day processes and requirements. For example, and not limited to:
 - Access – Finance and Budgeting System
 - Arbor – Management Information System
 - Crowe – Auditors
 - Computer Systems in Education (CSE) – IT Service Provider
 - CPOMS – Pupil Safeguarding Portal
 - Liberata – Payroll Provider
 - Randall & Payne – Auditors
 - Schools UK – Staff Absence (and Well-being) Provider
 - Teacher Pensions

Your personal information may be transferred outside the UK and the European Economic Area (EEA), including to the United States. Where information is transferred outside the UK or EEA to a country that is not designated as “adequate” in relation to data protection, the information is adequately protected by the use of International Data Transfer Agreements and security measure, and other appropriate safeguards. For more information on international transfers, please contact us at the details below.

6.7 Why we share school workforce information

We do not share information about our workforce members with anyone without consent unless the law and our policies allow us to do so.

6.7.1 Local Authority (Worcestershire County Council)

We are required to share information about our workforce members with our Local Authority (LA) under section 5 of the Education (Supply of Information about the School Workforce) (England) Regulations 2007 and amendments. This may include, inter alia matters relating to the following:

- Payroll
- Contracts
- Occupational Health

6.7.2 Department for Education (DfE)

We share personal data with the DfE on a statutory basis. We are required to share information about our school employees with the DfE under section 5 of the Education (Supply of Information about the School Workforce) (England) Regulations 2007 and amendments. All data is transferred securely and held by DfE under a combination of software and hardware controls which meet the current government security policy framework. For more information about the Department's data sharing process, please visit: <https://www.gov.uk/data-protection-how-we-collect-and-share-research-data>.

6.8 Freedom of Information Act and Environmental Information Regulations 2004

As a public body, our school is subject to requests made under the above legislation. Therefore, we have a legal obligation to process any personal data we hold when considering requests under these laws. For example, we may receive a request asking about numbers of staff with particular levels of professional qualification. However, we will never disclose personal data in our responses to these requests where to do so would contravene the principles of data protection.

6.9 Requesting access to your personal data

Under data protection legislation, you have the right to request access to information about you that we hold. To make a request for your personal information, contact the Head Teacher, the Director of Operations or the Data Protection Officer.

You also have the right to:

- Be informed about the collection and use of your personal data.
- Rectification, i.e. to have inaccurate personal data rectified, or completed if it is incomplete.
- Erasure, often known as the 'right to be forgotten'; however this does not apply where, amongst other things, processing is necessary to comply with a legal obligation.
- Restrict processing, although, as above this is a limited right.
- Object; though other than for marketing purposes, this is also limited as above.
- Where we rely on your consent to process your data, you have the right to withdraw that consent. If you do change your mind, or you are unhappy with our use of your personal data, please let us know.
- You also have rights in relation to automated decision making and profiling, though these are not currently relevant.
- The right to seek redress, either through the ICO, or through the courts.

6.10 How Government uses your data

The workforce data that we lawfully share with the DfE through data collections:

- Informs departmental policy on pay and the monitoring of the effectiveness and diversity of the school workforce.
- Links to school funding and expenditure.

- Supports 'longer term' research and monitoring of educational policy.

6.10.1 Data collection requirements

The DfE collects and processes personal data relating to those employed by schools (including Multi Academy Trusts) and local authorities that work in state funded schools (including all maintained schools, all academies and free schools and all special schools including Pupil Referral Units and Alternative Provision). All state funded schools are required to make a census submission because it is a statutory return under sections 113 and 114 of the Education Act 2005. To find out more about the data collection requirements placed on us by the Department for Education including the data that we share with them, go to <https://www.gov.uk/education/data-collection-and-censuses-for-schools>.

6.10.1 Sharing by the Department

The Department may share information about school employees with third parties who promote the education or well-being of children or the effective deployment of school staff in England by:

- Conducting research or analysis.
- Producing statistics.
- Providing information, advice or guidance.

The Department has robust processes in place to ensure that the confidentiality of personal data is maintained and there are stringent controls in place regarding access to it and its use. Decisions on whether DfE releases personal data to third parties are subject to a strict approval process and based on a detailed assessment of:

- Who is requesting the data.
- The purpose for which it is required.
- The level and sensitivity of data requested.
- The arrangements in place to securely store and handle the data.

To be granted access to school workforce information, organisations must comply with its strict terms and conditions covering the confidentiality and handling of the data, security arrangements and retention and use of the data.

If you need more information about how our local authority and/or DfE collect and use your information, please visit:

- <http://www.derbyshire.gov.uk/privacynotices> ; or
- <https://www.gov.uk/data-protection-how-we-collect-and-share-research-data>

6.11 Contact us

If you have a concern about the way we are collecting or using your personal data or you would like to discuss anything in this privacy notice, we ask that you raise your concern with us in the first instance.

Please contact the Head Teacher or School Data Protection Officer:

Data Protection Officer:	Education Data Hub (GDPR for Schools), Derbyshire County Council
DPO E-mail:	DPforschools@derbyshire.gov.uk
DPO Phone:	01629 532888

DPO Address: Room 396, North Block, County Hall, Smedley Street, Matlock,
Derbyshire. DE4 3AG

If however you are dissatisfied with our response to your concerns you can of course contact the ICO quoting our ICO registration number **ZA063714** and stating that the Data Controller is **Aspire Free School Academy Trust**
Information Commissioners' Office

Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

Tel: 0303 123 1113 (local rate) or 01625 545 745 if you prefer to use a national rate number
Fax: 01625 524 510

Website: <https://ico.org.uk/concerns/>

Appendix 7: Privacy Notice: Pupils & Family

7.1 How we use pupil information

We collect, hold, use and share information about our pupils and their families. This is known as “personal data” and you have rights around that data, including knowing how and why we are processing the data. “Processing” data means everything from collecting, to storing, using, sharing and disposing of it.

For the purposes of Data Protection legislation The Aspire Free School Academy Trust is a data controller and is registered as such with the Information Commissioner’s Office.

Our Data Protection Officer is **GDPR for Schools, Derbyshire County Council** (see ‘Contact us’ below).

7.2 The types of information we process

- Your name, unique pupil number and contact details including your address.
- Attendance records (sessions attended, number of absences, absence reasons and previous schools attended).
- Behavioural information (such as exclusions/suspensions).
- Assessment and attainment (such as National curriculum assessment results e.g. Key Stage 2 results, exam results and student performance at different data collections, post 16 courses enrolled for and any relevant results).
- Medical conditions we need to be aware of, including SEND, mental and physical health.
- Safeguarding information including court orders and/or social care involvement.
- For pupils enrolling for post 14 qualifications, the Learning Records Service will give us the unique learner number (ULN) and may also give us details about your learning or qualifications.
- Destination data (this is information about what pupils do after leaving the school, for example college, university, apprenticeship, employment).
- Post 16 learning information.
- Extra-curricular and enrichment participation
- CCTV data.
- Photographs of you.
- Correspondence and complaints.

7.2.1 Special Category data (sensitive information)

- Characteristics (including ethnicity and language).
- Safeguarding information (such as court orders and professional involvement).
- Special Educational needs (including the needs and ranking).
- Medical information that we need to be aware of (including your Doctor’s information, child health, dental health, allergies, medication and dietary requirements).
- Free school meal eligibility
- Other funding (Pupil Premium, High Needs Funding and Catch-Up Funding)

7.3 Why we collect and use your information

7.3.1 Pupil Information

We collect and use your information to:

- To support your learning

- To monitor and report on pupil attainment progress
- To provide appropriate pastoral care
- To assess the quality of our services
- To keep children safe
- photos are used for identification purposes (safeguarding), and celebration purposes (to record work, classes and school events)
- To meet the legal duties placed upon us by the Department for Education
- To comply with the law in general
- For site safety and security
- To protect against fraud
- To streamline systems

7.3.2 Family Information

We collect and use information about our pupils'

- To fulfil our legal obligations
- For the admissions process
- For communication and reporting purposes
- For safeguarding and welfare purposes
- To keep families informed about events and emergencies
- Gather feedback about our work

Under the General Data Protection Regulation (UK GDPR), the lawful bases we rely on for processing pupil and family information are:

- Article 6(a) – Your consent (for anything which does not fall into the purposes explained below).
- Article 6(c) – Compliance with our legal obligations as set out in the Education Act 1996 (as amended). We are required to share information about our pupils with the (DfE) under regulation 3 of The Education (Information About Individual Pupils) (England) Regulations 2013. In addition, there are extensive statutory obligations that a school is subject to – further details about these are available from our Data Protection Officer.
- Being necessary for us to carry out tasks that are in the Public Interest

The ways we collect and use sensitive pupil and family information are lawful based on: your explicit consent; for compliance with certain legal obligations, or for exercising certain legal rights; for protecting a person's vital interests in an emergency; for health and public health reasons; or for carrying out tasks that are in the substantial public interest including for safeguarding purposes.

Please see our Data Protection Policy document for full details of these lawful bases for processing this data.

7.3.3 Marketing purposes

Where a family member gives us consent, we may send them marketing information by text message or email, such as for promoting school events, campaigns or charities. Consent can be withdrawn at any time by contacting us (see the Contacts section).

7.3.4 Use of your child's data in automated decision making and profiling

We do not currently process any personal data through automated decision making or profiling. If this changes in the future, we will amend any relevant privacy notices in order to explain the processing to you, including your right to object to this.

7.4 How we collect pupil and family information

We collect pupil information using admission forms completed by referring schools and parent/carer when a pupil joins our school, data collection forms, CCTV cameras, information produced from our day-to-day interaction with pupils, and other information provided by; parents/carers, the previous school/provisions, local authorities, NHS, Police, the Department for Education (DfE) and by secure file transfer Common Transfer File (CTF).

Whilst most of the pupil information you provide to us is mandatory, some of it is requested on a voluntary basis. We will let you know, when we ask you for information, whether you are required to provide the information and your rights in relation to this.

7.5 How, where and for how long we store pupil and family information

We store pupil information securely on the School's IT network, backed up through Redstor. Secure storage is provided for paper based records.

We only keep the information for the length of time we need it for, as shown in our data retention schedule. For more information on our data retention schedule, please refer to Appendix 9 of this document.

We are currently following the instructions of the Independent Inquiry into Child Sexual Abuse (IICSA) which states that student records should not be destroyed until this inquiry is complete.

We dispose of personal information securely when we no longer need it.

7.6 Who we share pupil information with

We routinely share pupil information with:

- Referring (home) schools.
- Our local authority (Worcestershire County Council).
- Other relevant local authorities.
- Our Governing Body.
- Youth support services/careers services (pupils aged 13+).
- Post 16 destinations, for example further education schools and colleges.
- Employers/training providers where references are requested.
- Work experience providers.
- The Department for Education (DfE), including Learner Record Services and the National Pupil Database.
- Police.
- NHS (agencies and services)/School Nurse.
- External systems used by the School to carry out day to day processes and requirements. For example (but not limited to):
 - Arbor – Management Information System
 - Computer Systems in Education (CSE) – IT Service Provider
 - CPOMS – Pupil Safeguarding Portal
 - Crowe – External Auditor
 - Examination and Accreditation Awarding Organisations (e.g. Pearson, AQA etc.)
 - Group Call – Encrypted Data Exporter
 - Randall & Payne – External Auditor

7.7 International Transfers

Your personal information may be transferred outside the UK and the European Economic Area ('EEA'), including to the United States. Where information is transferred outside the UK or EEA to a country that is not designated as "adequate" in relation to data protection law, the information is adequately protected by the

use of International Data Transfer Agreements and security measures, and other appropriate safeguards. For more information on international transfers please contact us at the details below.

7.8 Freedom of Information Act and Environmental Regulations 2004

As a public body, our school is subject to requests made under the above legislation. However, we will never disclose personal data in our responses to these requests where to do so would contravene the principles of data protection.

7.9 Why we regularly share pupil information

We do not share information about our pupils with anyone without consent unless the law and our policies allow us to do so.

7.9.1 Youth Support Services and Careers advisors

Pupils aged 13+

Once our pupils reach the age of 13, we pass information about the pupil to our local authority so they can carry out their legal responsibilities in relation to the education or training of 13-19 year olds under section 507B of the Education Act 1996.

This enables them to provide services as follows:

- youth support services
- careers advisers

A parent or guardian can object to any information in addition to their child's name, address and date of birth being passed to their local authority or provider of youth support services by informing us. This right is transferred to the pupil once they reach the age 16.

Data is securely transferred to the youth support service under the terms of a Data Sharing Agreement.

For more information about services for young people, please visit our local authority website or contact our Schools' Data Protection Officer.

Pupils aged 16+

We will also share certain information about pupils aged 16+ with our local authority as they have responsibilities in relation to the education or training of 13-19 year olds under section 507B of the Education Act 1996.

This enables them to provide services as follows:

- post-16 education and training providers
- youth support services
- careers advisers

A pupil once they reach the age of 16 can object to information other than their name, address and date of birth being passed to their local authority by contacting us.

For more information about services for young people, please visit our local authority website.

7.9.2 Department for Education

The Department for Education (DfE) collects personal data from educational settings and local authorities via various statutory data collections. We are required to share information about our pupils with the Department

for Education (DfE) either directly or via our local authority for the purpose of those data collections, under: Regulation 5 of The Education (Information About Individual Pupils) (England) Regulations 2013.

7.9.3 Local Authorities

We may be required to share information about our pupils with the local authority to ensure that they can conduct their statutory duties.

7.10 Requesting access to your personal data and other rights

Under data protection law, pupils have the right to request access to information about them that we hold, and in some cases, parents can make the request on the pupil's behalf, although this will be subject to the pupil's consent if they are deemed to be competent to understand the request and any implications.

Family members/carers also have the right to request access to information about them that we hold.

You also have the right to:

- Be informed about the collection and use of your personal data.
- Have inaccurate personal data changed, or completed if it is incomplete.
- Erasure, often known as the 'right to be forgotten'; however this does not apply where, amongst other things, processing is necessary to comply with a legal obligation.
- Restrict the way we are using your information, although, as above this is a limited right.
- Object to the way we are using your information; though other than for marketing purposes, this is also limited as above.
- Where we rely on your consent to collect and use your data, you have the right to withdraw that consent. If you do change your mind, or you are unhappy with our use of your personal data, please let us know – see our contacts at the end of this document.
- You also have rights in relation to automated decision making and profiling, though these are not currently relevant as we don't carry out automated decision making or profiling.
- Finally, the right to complain about the way we use your personal information to the ICO, or to seek compensation through the courts.

If you would like to request access to your data, or use any of the other rights listed above, please contact the Head Teacher in the first instance.

7.11 How Government uses your information

The pupil data that we lawfully share with the DfE through data collections:

- Underpins school funding, which is calculated based upon the numbers of children and their characteristics in each school.
- Informs 'short term' education policy monitoring and school accountability and intervention (for example, school GCSE results or Pupil Progress measures).
- Supports 'longer term' research and monitoring of educational policy (for example how certain subject choices go on to affect education or earnings beyond school)

7.11.1 Data collection requirement

To find out more about the data collection requirements placed on us by the Department for Education (for example; via the school census) go to <https://www.gov.uk/education/data-collection-and-censuses-for-schools>

7.11.2 The National Pupil Database (NPD)

Much of the data about pupils in England goes on to be held in the National Pupil Database (NPD). The NPD is owned and managed by the Department for Education and contains information about pupils in schools in England. It provides invaluable evidence on educational performance to inform independent research, as well as studies commissioned by the Department.

It is held in electronic format for statistical purposes. This information is securely collected from a range of sources including schools, local authorities and awarding bodies.

To find out more about the NPD, go to <https://www.gov.uk/government/publications/national-pupil-database-user-guide-and-supporting-information>

7.11.3 Sharing by the Department

The law allows the Department to share pupils' personal data with certain third parties, including:

- schools
- local authorities
- researchers
- organisations connected with promoting the education or wellbeing of children in England
- other government departments and agencies
- organisations fighting or identifying crime

For more information about the Department's NPD data sharing process, please visit:

<https://www.gov.uk/data-protection-how-we-collect-and-share-research-data>

Organisations fighting or identifying crime may use their legal powers to contact DfE to request access to individual level information relevant to detecting that crime. Whilst numbers fluctuate slightly over time, DfE typically supplies data on around 600 pupils per year to the Home Office and roughly 1 per year to the Police.

For information about which organisations the Department has provided pupil information, (and for which project) or to access a monthly breakdown of data share volumes with Home Office and the Police please visit the following website: <https://www.gov.uk/government/publications/dfe-external-data-shares>

7.11.4 Learner Records Service

The information you supply is used by the Learning Records Service (LRS). The LRS issues Unique Learner Numbers (ULN) and creates Personal Learning records across England, Wales and Northern Ireland, and is operated by the Education and Skills Funding Agency, an executive agency of the Department for Education (DfE). For more information about how your information is processed, and to access your Personal Learning Record, please refer to: <https://www.gov.uk/government/publications/lrs-privacy-notice>

7.11.5 How to find out what personal information the DfE hold about you

Under the terms of the Data Protection Act 2018, you are entitled to ask the Department:

- If they are processing your personal data.

- For a description of the data they hold about you.
- The reasons they're holding it and any recipient it may be disclosed to.
- For a copy of your personal data and any details of its source.

If you want to see the personal data held about you by the Department, you should make a 'subject access request'. Further information on how to do this can be found within the Department's personal information charter that is published at the address below:

<https://www.gov.uk/government/organisations/department-for-education/about/personal-information-charter>

To contact DfE: <https://www.gov.uk/contact-dfe>

7.12 Contact us

If you have a concern about the way we are collecting or using your personal data or you would like to discuss anything in this privacy notice, we ask that you raise your concern with us in the first instance.

Please contact the Head Teacher or School Data Protection Officer:

Data Protection Officer:	Education Data Hub (GDPR for Schools), Derbyshire County Council
DPO E-mail:	DPforschools@derbyshire.gov.uk
DPO Phone:	01629 532888
DPO Address:	Room 396, North Block, County Hall, Smedley Street, Matlock, Derbyshire. DE4 3AG

If however you are dissatisfied with our response to your concerns you can of course contact the ICO quoting our ICO registration number **ZA063714** and stating that the Data Controller is **Aspire Free School Academy Trust**

Information Commissioners' Office

Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

Tel: 0303 123 1113 (local rate) or 01625 545 745 if you prefer to use a national rate number
Fax: 01625 524 510

Website: <https://ico.org.uk/concerns/>

Appendix 8: Privacy Notice: School Governors

8.1 How we use governors' information

We collect, hold, use and share information about our workforce. This is known as “personal data” and you have rights around that data, including knowing how and why we are processing the data. “Processing” data means everything from collecting, to storing, using, sharing and disposing of it. We collect, hold and share personal data on the School Governors.

For the purposes of Data Protection legislation The Aspire Free School Academy Trust is a data controller and is registered as such with the Information Commissioner's Office.

Our Data Protection Officer is **GDPR for Schools, Derbyshire County Council** (see 'Contact us' below).

8.2 The categories of governors' information that we process include

- Personal identifiers, contacts and characteristics (such as name, date of birth, contact details, address and photograph).
- Governance details (such as role, start and end dates).
Information about medical or health conditions, that we need to know about, including whether you have a disability for which the school needs to make reasonable adjustments*

We may also collect, use and store information about criminal convictions, offences and prohibitions. This information may have come from other organisations including former employers, Teacher Regulation Agency, social services and the Disclosure & Barring Service.

8.3 Why we collect and use governors' information

The personal data collected is essential, in order for the school to fulfil their official functions and meet legal requirements.

We collect and use governance information, for the following purposes:

- a) To meet the statutory duties placed upon us.
- b) Facilitate safer recruitment (e.g. by carrying out criminal records checks).
- c) To help us to deliver our responsibilities to our school community.
- d) To communicate with our Governing Body.
- e) To inform the school community of the identity of the individuals who comprise the Governing Body.
- f) Photographic images for identification purposes (safeguarding and identifying Governors to our parents and pupils), and celebration purposes (to record school events).

Under the General Data Protection Regulation (UK GDPR), the legal basis we rely on for processing personal information for general purposes are:

- Article 6(a) – Your consent (for any processing which does not fall into the other bases explained below)
- Article 6(c) - Compliance and with our legal obligations
- Article 6(e) – Carrying out tasks in the Public Interest.

All academy trusts, under Academies Financial Handbook have a legal duty to provide the information as detailed above.

The ways we collect and use sensitive information about governors are lawful based on: your explicit consent; for compliance with certain legal obligations, or for exercising certain legal rights; for protecting a person's vital interests in an emergency; for health and public health reasons; or for carrying out tasks that are in the substantial public interest including for safeguarding purposes. Please refer to the Data Protection Policy document for full details of these lawful bases for processing this data.

Types of data that are special category are indicated above by *.

8.3.1 Marketing Purposes

Where you have given us consent to do so, we may send you marketing information by text message or email promoting school events, campaigns and or charities. You can withdraw this consent at any time by contacting us (see the Contacts section).

8.3.2 Automated decision making & profiling

We do not currently process any personal data through automated decision making or profiling. Should this change in the future, privacy notices will be updated to explain both the processing and your right to object to it.

8.4 How we collect governors' information

We collect personal information in a variety of ways. For example, data is collected through application forms, obtained from your passport or other identity documents such as your driving licence, from forms completed by you at the start of or during your term as a Governor, from correspondence with you, or through interviews, meetings or other assessments, images provided by you or taken using school photographic equipment, local authorities, the NHS, the Police, the Disclosure and Barring Service and the Department for Education.

Governors' data is essential for the school's operational use. Whilst the majority of personal information you provide to us is mandatory, some of it may be requested on a voluntary basis. In order to comply with GDPR, we will inform you at the point of collection, whether you are required to provide certain information to us or if you have a choice in this.

8.5 How, where and for how long we store governor's information

We store governor information securely on the School's IT network, backed up through Redstor. Secure storage is provided for paper based records.

We only keep the information for the length of time we need it for, as shown in our data retention schedule. For more information on our data retention schedule, please refer to Appendix 9 of this document.

We dispose of personal information securely when we no longer need it.

8.6 Who we share governors' information with

We routinely share this information with:

- Our Local Authority (Worcestershire County Council)
- The Department for Education
- Company House
- Our Governing Body
- The Disclosure and Barring Service
- GovernorHub (The Key for School Governors)
- Entrust (Clerking service provider)

- Our school community (via the school website)

8.7 Why we share governors' information

We do not share information about our Governors with anyone without consent unless the law and our policies allow us to do so.

8.8 Local Authority

Where we are required to share information about school governance with our Local Authority we do so under the terms of a Data Sharing Agreement viewable at <https://schoolsnet.derbyshire.gov.uk/administration-services-and-support/information-governance/information-sharing.aspx>

8.9 Department for Education

We share personal data with the Department for Education (DfE) on a statutory basis. We are required to share information about our governors with the Department for Education (DfE) under Section 538 of the Education Act 1996.

8.10 Freedom of Information Act and Environmental Information Regulations 2004

As a public body, our school is subject to requests made under the above legislation. Therefore, we have a legal obligation to process any personal data we hold when considering requests under these laws.

For example, we may receive a request asking about numbers and/or roles of governors.

However, we will never disclose personal data in our responses to these requests where to do so would contravene the principles of data protection.

8.11 Requesting access to your personal data

Under data protection legislation, you have the right to request access to information about you that we hold. To make a request for your personal information, contact the School Office, the Headteacher or the Data Protection Officer.

You also have the right to:

- Be informed about the collection and use of your personal data.
- Rectification, i.e. to have inaccurate personal data rectified, or completed if it is incomplete.
- Erasure, often known as the 'right to be forgotten'; however this does not apply where, amongst other things, processing is necessary to comply with a legal obligation.
- Restrict processing, although, as above this is a limited right.
- Object; though other than for marketing purposes, this is also limited as above.
- Where we rely on your consent to process your data, you have the right to revoke that consent. If you do change your mind, or you are unhappy with our use of your personal data, please let us know – our contacts are at the end of this document.
- You also have rights in relation to automated decision making and profiling, though these are not currently relevant.
- Finally, the right to seek redress, either through the ICO, or through the courts

8.12 How Government uses your data

The governance data that we lawfully share with the DfE via Get Information About Schools (GIAS) (<https://get-information-schools.service.gov.uk/>):

- Will increase the transparency of governance arrangements.

- Will enable academy trusts and the department to identify more quickly and accurately individuals who are involved in governance and who govern in more than one context.
- Allows the department to be able to uniquely identify an individual and in a small number of cases conduct checks to confirm their suitability for this important and influential role.

Note: Some of these personal data items are not publicly available and are encrypted within the GIAS system. Access is restricted to a small number of DfE staff who need to see it in order to fulfil their official duties. The information is for internal purposes only and not shared beyond the department, unless law allows it.

8.13 Sharing by the Department of Education

The Department for Education (DfE) collects personal data from educational settings and local authorities. We are required to share information about individuals in governance roles with the Department for Education (DfE), under the requirements set out in the Academies Financial Handbook .

All data is entered manually on the GIAS system and held by DfE under a combination of software and hardware controls which meet the current government security policy framework.

To find out more about the data collection requirements placed on us by the Government and the Department for Education including the data that we share with them, go to www.gov.uk/government/news/national-database-of-governors.

8.14 Contact us

If you have a concern about the way we are collecting or using your personal data or you would like to discuss anything in this privacy notice, we ask that you raise your concern with us in the first instance.

Data Protection Officer:	GDPR for Schools, Derbyshire County Council
DPO E-mail:	DPforschools@derbyshire.gov.uk
DPO Phone:	01629 532888
DPO Address:	Room 396, North Block, County Hall, Smedley Street, Matlock, Derbyshire. DE4 3AG

If however you are dissatisfied with our response to your concerns you can of course contact the ICO quoting our ICO registration number **ZA063714** and stating that the Data Controller is **Aspire Free School Academy Trust**.

Information Commissioners' Office

Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

Tel: 0303 123 1113 (local rate) or 01625 545 745 if you prefer to use a national rate number
Fax: 01625 524 510

Website: <https://ico.org.uk/concerns/>

Appendix 9: Retention and Deletions Policy

9.1 Introduction

The Independent Inquiry into Child Sexual Abuse (IICSA) states: *“Institutions have an obligation to preserve records for the Inquiry for as long as necessary to assist the Inquiry. Prolonged retention of personal data by an organisation at the request of the Inquiry would not therefore contravene data protection legislation, provided **such information is restricted to that necessary to fulfil any potential legal duties that organisation may have in relation to the Inquiry.** An institution may have to account for its previous activities to the Inquiry so retention of the data will be regarded as necessary for this purpose.”*

Therefore, any records that may be in scope of the inquiry because they pertain to matters relating to the care or abuse of children should be retained until further notice and the periods specified in this guidance, in relation to those records only, are suspended until further notice.

This record retention and deletion policy contains recommended retention periods for the different record series created and maintained by The Aspire Academy. The schedule refers to all information whether it is held in hard copy or electronic format including cloud and web based or on third party platforms.

Some of the retention periods are governed by statute. Others are guidelines, following best practice, employed by schools throughout the United Kingdom. Every effort has been made to ensure that these retention periods are compliant with the requirements of the UK General Data Protection Regulation 2018 (GDPR), the Data Protection Act 2018 (DPA), Article 8, the Human Rights Act 1998, the Freedom of Information Act 2000 (FOI) and the Code of Practice on Records Management (under Section 46 of the FOI).

Managing records series using these retention guidelines will be deemed to be ‘normal processing’ under the terms of the legislation noted above. If those record series are to be kept for longer or shorter periods than the time scales held in this document, the reasons for any deviation must be recorded.

9.2 Purpose

This policy, for managing records at The Aspire Academy has been drawn up in conformity with legislation, regulations affecting schools and best practice as promoted by the Information and Records Management Society of Great Britain.

This policy sets out guidelines for recording, managing, storing and the disposal of data, whether they are held on paper or electronically (including online), in order to assist staff, and the school, to comply with the General Data Protection Regulation (EU) 2016/679 (GDPR) including as adopted by the United Kingdom as a result of its exit from the European Union (“UK GDPR”), Data Protection Act 2018 and the Freedom of Information Act 2000. It should be read and used in conjunction with all of our related policies.

It is expected that;

- All information held by schools needs to be justifiable, by reference, to its purpose.
- Schools must be transparent and accountable as to what data they hold.
- Schools must understand and explain the reasons why they hold data.
- Schools must be able to respond to Subject Access Requests.
- Schools must be able to amend, delete or transfer data promptly upon any justified request.
- Schools must be able to audit how personal data was collected and when and why.
- Schools must hold sensitive data securely, accessed only by those with reason to view it and possess a policy as to why it is needed.

9.3 Disposal of Data

Article 5(e) of the GDPR states that personal data should be 'kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes... in order to safeguard the rights and freedoms of the data subject ('storage limitation')'.

Not all data needs to be destroyed. The school should determine whether records are to be selected for permanent preservation, or for destruction or to be transferred into a different format.

When information is no longer required, it should be disposed of. For confidential, sensitive or personal information, to be considered securely disposed of, it must be in a condition where it cannot either be read or reconstructed.

- Skips, 'regular' waste disposal and ribbon shredders are not secure.
- Paper records should be cross-shredded, incinerated, or pulped.
- CDs/DVDs/discs should be cut into pieces.
- Hard copy images, AV recordings and hard disks should be dismantled and destroyed.
- Where third party disposal companies are employed, a certificate of destruction must be obtained.
- Staff working for external provider should have been trained in the handling and destruction of confidential data.

If the school receives a request for records that have not yet been destroyed, even if they should have been destroyed, that record must still be made available to the requestor.

The Freedom of Information Act 2000 requires the school to maintain a list of all records that have been destroyed and who authorised their destruction. This record should be retained for 15 years. The appropriate members of staff (Data Lead) should record:

- File reference and/or unique identifier (if appropriate)
- Title or brief description of contents
- Number of files
- Name of the authorising officer

9.4 Transfer of records to Archives

A school archive is different from official school records. A school archive preserves data where there is a legitimate interest in holding that information e.g. to commemorate a significant event in the life of the school. It can take on many characteristics and serve many purposes, but it neither complements nor replaces the official record-keeping systems.

Where records have been identified as being worthy of permanent preservation, due to their historical or social value, they may be retained on site or transferred to the Local Authority Record Office (see local guidance [Find an archive | The National Archives](#)).

Where the school decides to maintain an onsite archive, the school should consult with their Data Protection Officer to implement the following steps:

- Establish what information needs to be archived
- Select someone to serve as the archivist. This may be an additional function within an established role, to work alongside both the Data Protection Officer and Data Lead officer (where applicable).
- Select a physical location to house the collection, and determine what equipment and supplies are needed to accomplish the project for the first year and on a continuing basis e.g. safe storage, shelving
- Remember that archives can include electronic data e.g. schools may have digital photographs which are no longer displayed on their website or social media pages. Consider not only holding and

cataloguing this data in a secure driver, but making potential requestors aware of its presence, through a dedicated website.

- Come to an agreement with the Local Authority Record Office, in order for the collected materials could be turned over if the school archives should be discontinued.

9.5 Transfer of records to other Media

Where lengthy retention periods have been allocated to records, the school will consider converting paper records to other media (e.g. digital or virtual, 'cloud' based). The lifespan of the media, and the ability to migrate data, should be documented in a Digital Continuity Policy. Where this is undertaken a scanning risk assessment will be undertaken to ensure the procedure is adequate.

9.6 Transfer of records to other settings and 'last known school'

When a pupil leaves the school, all necessary pupil records should be transferred in a secure manner. If the records contain sensitive information (e.g. Child Protection records), proof of receipt must be obtained and logged by the school's Designated Safeguarding Lead. All data held by the school should then be deleted, including all paper records and data stored electronically. A record should be kept for tracking and auditing purposes only. Responsibility for maintaining the pupil record passes to the 'last known school'.

The school is the final or last known school if:

- Secondary phase and the pupil left at 16 years old or for post-16 or independent education, or
- At any point the pupil left for elective home education, they are missing from education, or have left the UK, or have died.

The Pupil Record should be retained as a whole for 25 years from the date of birth of the pupil, after which time, if no longer required, it can be deleted or destroyed.

SEN and other support service records can be retained for a longer period of 31 years to enable defence in a "failure to provide a sufficient education" case.

If a school wishes to retain data for analysis or statistical purposes, it should be done in an anonymised fashion.

9.7 Responsibility and Monitoring

The Head Teacher (or as delegated) holds primary and day to day responsibility, for implementing this policy. The Data Protection Officer, in conjunction with the school, is responsible for monitoring its use and effectiveness and resolving any queries with regards the interpretation of the policy. All permissions to access data are granted by the Head Teacher and recorded in the member of staff's personnel file.

All members of staff, with access to records, are expected to;

- Manage their current record keeping systems using the Retention Policy.
- Only dispose of records in accordance with the requirements outlined in this policy, if authorised to do so.
- Ensure that any proposed divergence from the records retention schedule and disposal policies is authorised and documented by the Head Teacher.

This policy does not form part of any employee's contract of employment and is not intended to have a contractual effect. However, it does reflect the school's current practice, the requirements of current legislation and best practice and guidance. It may be amended by the school but any changes will be notified to employees within one month of the date on which the change is intended to take effect. The school may also vary any parts of the procedure, including time limits, as appropriate.

9.8 Retention Table

The following list of documents is not exclusive. If you cannot find your document category amongst those listed below, please seek advice from the Head Teacher (or delegated representative) for DPO.

Description	Retention Period	Notes
Head Teacher and SLT		
Minutes of SLT and other meetings	Meeting Date + 3 years	May be Data Protection issues if minutes/reports/records/correspondence refer to individual pupils or members of staff
Reports created by Head Teacher or Management Team	Report Date + 3 years (minimum)	
Records created by Head, Deputy, Year Heads and others with administrative responsibilities	Current Academic Year + 6 years	
Correspondence created by Head, Deputy, Year Heads and others with administrative responsibilities	Date of Correspondence + 3 years	
Professional Development Plans	Life of plan + 6 years	
Admissions & Attendance		
Successful referral applications	Date of admission + 1 year	Data collected through Referral Forms – Original referral form kept on pupil file
Register of referral applications	Date of admission + 3 years	
Proof of parental address on admission	Current Year + 1 year	
Supplementary Information on admission		Added to pupil file
Unsuccessful referral applications	End of Academic year	
Attendance Registers	3 years +	Every entry must be preserved for a period or 3 years after the date on which the entry was made
Operational Administration		
Visitor books and signing in sheets	Current Year+ 6 years	
Recruitment & Operational Staff Management		
All records leading to Head Teacher appointment	Appointment date + 6 years	
All records leading to appointment of new member of staff: Successful candidates	Information added to employee personnel file	
All records leading to appointment of new member of staff: Unsuccessful candidates	Appointment date + 6 months	
Pre-employment vetting: DBS, identification		Any copied DBS certificates and ID documentation is shredded as soon as DBS application is made
Staff Personnel Files	Termination of employment + 6 years	
Timesheets	Current year + 6 years	

Annual appraisal/performance management	Current year + 5 years	
Disciplinary & Grievance Management		
Allegation of a child protection nature against a member of staff (including where unfounded)	Until person's normal retirement age or 10 years from date of allegation, whichever is longer.	Allegations found to be malicious should be removed from personnel files. If kept on file, a copy should be given to person concerned
Disciplinary Proceedings: Oral warning and first written warning	Date of warning + 6 months	If kept on Personnel File, they must be removed
Disciplinary Proceedings: second written warning	Date of warning + 12 months	
Disciplinary Proceedings: Oral warning and first written warning	Date of warning + 18 months	
Case not found	If incident is child protection related see above, else dispose at conclusion of the case.	
Health & Safety		
Records relating to accident & injuries at work	Date of incident + 12 years	Longer retention period for serious incidents
Accident reporting: Adults	Date of incident + 6 years	
Accident reporting: Children	Dob of child + 25 years	
Payroll and Pensions		
Maternity Pay	Current year + 3 years	
Retirement Benefits	Current year + 6 years	
Pupil Educational Records & Management Information		
Pupil's Educational Record	Date of Birth + 25 years	
Examination Results		Added to Pupil File Uncollected certificates should be returned to the examination board
Examination Results (School's Copy)	Current year + 6 years	
Child Protection information held on pupil file		MUST BE SHREDDED Child protection issues placed on pupil file should be in a sealed envelope (DoB + 25 years)
Child Protection information held in separate file	Date of Birth + 25 years	MUST BE SHREDDED This retention period agreed in consultation with Safeguarding Children Group on the understanding that the principal copy of this information will be found on the Local Authority Social Services record.
Published Admission Number (PAN) Reports, Value Added and Contextual Data, Self-Evaluation Forms	Current year + 6 years	

Parental consent forms for school trips where there has been no major incident	Conclusion of trip	
Parental consent forms for school trips where there has been major incident	Date of Birth of the pupil involved + 25 years	Retain permission slips of all pupils to evidence that correct procedures have been followed for all pupils.
Implementation of the Curriculum		
Schemes of Work, Timetable, Class Record Books, Mark Books, Record of Homework Set, Pupils' Works	Current year + 1	Secure Disposal
Special Educational Needs		
SEN files, reviews and individual ECHP	Date of Birth + 25 years Normally held on pupil file	Minimum period of retention. May keep for longer to defend against "failure to provide a sufficient education" case.
Statement and any amendments		
Advice and information provided to parents regarding educational needs		
Accessibility Strategy		