Larwood Academy Trust

Chair of Trustees: Daniel Login |BA (Hons)|
LARWOOD DRIVE, STEVENAGE, HERTFORDSHIRE, SG1 5BZ
Email: admin@larwood.herts.sch.uk **Telephone**: 01438 236333
Website: www.larwood.herts.sch.uk

Larwood School
Executive Headteacher: Mr Pierre van der Merwe |BA, NPQH|

Brandles School
Headteacher: Mr Paul Smith |BA (Hons), PGCE, NPQH|

Version Control

V1.1	November 2023	Added Appendix 1 and 2

Larwood Academy Trust

Chair of Trustees: Daniel Login |BA (Hons)|
LARWOOD DRIVE, STEVENAGE, HERTFORDSHIRE, SG1 5BZ
Email: admin@larwood.herts.sch.uk **Telephone**: 01438 236333
Website: www.larwood.herts.sch.uk

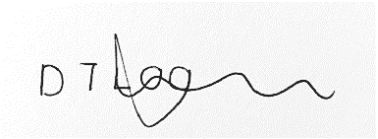
Larwood School
Executive Headteacher: Mr Pierre van der Merwe |BA, NPQH|

Brandles School
Headteacher: Mr Paul Smith |BA (Hons), PGCE, NPQH|

Dan Login
Chair of Trustees

Pierre van der Merwe
Executive Headteacher

DATA PROTECTION POLICY



Policy Number: 03
Review Committee: Finance and Resources
Type of Policy: Statutory
Review Period: Annually
Approved: November 2023
Next Review: November 2024

CONTENTS

1.AIMS

Our school aims to ensure that all personal data collected about staff, pupils, parents, governors, trustees, visitors and other individuals is collected, stored and processed in accordance with the General Data Protection Regulation (GDPR) and the expected provisions of the Data Protection Act 2018 (DPA 2018) as set out in the Data Protection Bill.

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

2. LEGISLATION AND GUIDANCE

This policy meets the requirements of the Data Protection Act 1998, and is based on guidance published by the Information Commissioner's Office, model privacy notices published by the Department for Education and Data protection guidance (DfE) Feb 2023
It also takes into account the expected provisions of the General Data Protection Regulation(UK GDPR, which is new legislation due to come into force in 2018.
In addition, this policy complies with regulation 5 of the Education (Pupil Information) (England) Regulations 2005, which gives parents the right of access to their child's educational record. It also reflects the ICO's code of practice for the use of surveillance cameras and personal information.

This policy complies with our funding agreement and articles of association.

Good data protection practices ensure that an organisation and the individuals within it can be trusted to collect, store and use our personal data fairly, safely and lawfully.

3.DEFINITIONS

Term	Definition
Personal data	Any information relating to an identified, or identifiable, individual. This may include the individual's: • Name (including initials) • Identification number • Location data • Online identifier, such as a username It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.
Special categories of personal data	Personal data which is more sensitive and so needs more protection, including information about an individual's: • Racial or ethnic origin • Political opinions

	• Religious or philosophical beliefs • Trade union membership • Genetics • Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes • Health – physical or mental • Sexual matters or sexual orientation
Processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.
Data subject	The identified or identifiable individual whose personal data is held or processed.
Data controller	A person or organisation that determines the purposes and the means of processing of personal data.
Data processor	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

4. THE DATA CONTROLLER

Our school processes personal information relating to pupils, staff and visitors, and, therefore, is a data controller.
The school is registered as a data controller with the Information Commissioner's Office and renews this registration annually.

5. ROLES AND RESPONSIBILITIES

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

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

5.2 Data protection officer
The data protection officer (DPO) is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable.
They will provide an annual report of their activities directly to the governing board and, where relevant, report to the board their advice and recommendations on school data protection issues.
The DPO is also the first point of contact for individuals whose data the school processes, and for the ICO.
Full details of the DPO's responsibilities are set out in their job description.
Our DPO is Carol Corol Connelly/Patrick Aikman of Schools DPO Service and is contactable via www.schoolsdposervice or carol@schoolDPOservice.com or patrick@schoolDPOservice.com or 07805 382374

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

5.4 All staff
Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Informing the school of any changes to their personal data, such as a change of address
- Contacting the DPO in the following circumstances:
- With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
- If they have any concerns that this policy is not being followed
- If they are unsure whether or not they have a lawful basis to use personal data in a particular way
- If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the European Economic Area
- If there has been a data breach
- Whenever they are engaging in a new activity that may affect the privacy rights of individuals
- If they need help with any contracts or sharing personal data with third parties

6. DATA PROTECTION PRINCIPLES

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

- Those principles are:

- lawfulness, fairness and transparency
- purpose limitation
- data minimisation
- accuracy
- storage limitation
- integrity and confidentiality (security)
- accountability

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

7. COLLECTING PERSONAL DATA

7.1 Lawfulness, fairness and transparency
We will only process personal data where we have one of 6 'lawful bases' (legal reasons) to do so under data protection law:
The lawful bases for processing are set out in Article 6 of the UK GDPR. At least one of these must apply whenever you process personal data:

Consent: the individual has given clear consent for you to process their personal data for a specific purpose.

Contract: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.

Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations).

Vital interests: the processing is necessary to protect someone's life.

Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

Legitimate interests: the processing is necessary for your legitimate interests or the legitimate interests of a third party, unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks.)

For special categories of personal data, we will also meet one of the special category conditions for processing which are set out in the GDPR and Data Protection Act 2018.

7.2 Limitation, minimisation and accuracy
We will only collect personal data for specified, explicit and legitimate reasons. We will explain these reasons to the individuals when we first collect their data.
If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so, and seek consent where necessary.
Staff must only process personal data where it is necessary in order to do their jobs.

When staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with the school's (record retention schedule/records management policy)

7.3 Storage limitations
We do not keep personal data for longer than required.
We periodically review the data we hold, and erase or anonymise it when no longer need it.
Individuals have a right to request any erasure of data if you no longer needed.
We only keep personal data for longer if we are keeping it for public interest archiving, scientific or historical research, or statistical purposes.

7.4 Integrity and confidentiality(security)
We undertake an analysis of the risks presented by our processing and use this to assess the appropriate level of security we need to put in place. When deciding what measures to implement, we take account of the state of the art and costs of implementation.

We have assessed what we need to do by considering the security outcomes we want to achieve. We have put in place basic technical controls such as those specified by established frameworks like Cyber Essentials.

We understand that we may also need to put other technical measures in place depending on our circumstances and the type of personal data we process. We use encryption and/or pseudonymisation where it is appropriate to do so.

We understand the requirements of confidentiality, integrity and availability for the personal data we process. We make sure that we can restore access to personal data in the event of any incidents, such as by establishing an appropriate backup process.

We conduct regular testing and reviews of our measures to ensure they remain effective, and act on the results of those tests where they highlight areas for improvement. Where appropriate, we implement measures that adhere to an approved code of conduct or certification mechanism.

7.5 Accountability
We take responsibility for complying with the UK GDPR, at the highest management level and throughout our organisation.
We put in place appropriate technical and organisational measures, such as:

Adopting and implementing data protection policies, taking a 'data protection by design and default' approach - putting appropriate data protection measures in place throughout the entire lifecycle of our processing operations, implementing appropriate security measures; recording and, where necessary, reporting personal data breaches; carrying out data protection impact assessments for uses of personal data that are likely to result in high risk to individuals' interests; adhering to relevant codes of conduct

We review and update our accountability measures at appropriate intervals.

8. SHARING PERSONAL DATA

We will not normally share personal data with anyone else, but may do so where:

- There is an issue with a pupil or parent/carer that puts the safety of our staff at risk.
- We need to liaise with other agencies – we will seek consent as necessary before doing this.
- Our suppliers or contractors need data to enable us to provide services to our staff and pupils – for example, IT companies. When doing this, we will:
- Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law.
- Establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data we share.
- Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us

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

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

We may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of our pupils or staff.
Where we transfer personal data to a country or territory outside the European Economic Area, we will do so in accordance with data protection law.

8.1 Pupils and parents

We hold personal data about pupils to support teaching and learning, to provide pastoral care and to assess how the school is performing. We may also receive data about pupils from other organisations including, but not limited to, other schools, local authorities and the Department for Education.
This data includes, but is not restricted to:

- Contact details
- Results of internal assessment and externally set tests
- Data on pupil characteristics, such as ethnic group or special educational needs
- Exclusion information
- Details of any medical conditions

We will only retain the data we collect for as long as is necessary to satisfy the purpose for which it has been collected.

We will not share information about pupils with anyone without consent unless the law and our policies allow us to do so. Individuals who wish to receive a copy of the information that we hold about them/their child should refer to sections 8 and 9 of this policy.
We are required, by law, to pass certain information about pupils to specified external bodies, such as our local authority and the Department for Education, so that they are able to meet their statutory obligations.

8.2 Staff
We process data relating to those we employ to work at, or otherwise engage to work at, our school. The purpose of processing this data is to assist in the running of the school, including to:

- Enable individuals to be paid
- Facilitate safe recruitment
- Support the effective performance management of staff
- Improve the management of workforce data across the sector
- Inform our recruitment and retention policies
- Allow better financial modelling and planning
- Enable ethnicity and disability monitoring
- Support the work of the School Teachers' Review Body
- Staff personal data includes, but is not limited to, information such as:
- Contact details
- National Insurance numbers
- Salary information and contracts
- Qualifications and CPD reviews
- Absence data
- Personal characteristics, including ethnic groups
- Medical information
- Outcomes of any disciplinary procedures

We will only retain the data we collect for as long as is necessary to satisfy the purpose for which it has been collected.
We will not share information about staff with third parties without consent unless the law allows us to.
We are required, by law, to pass certain information about staff to specified external bodies, such as our local authority and the Department for Education, so that they are able to meet their statutory obligations.
Any staff member wishing to see a copy of information about them that the school holds should contact the Business Manager in the first instance.

9. SUBJECT ACCESS REQUESTS

If staff are given this request directly, they need to pass on this request to the Headteacher, Deputy Headteacher or Business Manager, who will then ensure that it is passed onto the DPO.

Subject access requests

Individuals have a right to make a 'subject access request' to gain access to personal information that the school holds about them. This includes:

- Confirmation that their personal data is being processed
- Access to a copy of the data
- The purposes of the data processing
- The categories of personal data concerned
- Who the data has been, or will be, shared with
- How long the data will be stored for, or if this isn't possible, the criteria used to determine this period
- The source of the data, if not the individual
- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual

Subject access requests must be submitted in writing, either by letter, email or fax to the DPO. They should include:

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

9.1 Children and subject access requests

Children below the age of 12 are generally not regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of pupils at our school may be granted without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

9.2 Responding to subject access requests

- When responding to requests, we:
- May ask the individual to provide 2 forms of identification
- May contact the individual via phone to confirm the request was made
- Will respond without delay and within 1 month of receipt of the request
- Will provide the information free of charge
- May tell the individual we will comply within 3 months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within 1 month, and explain why the extension is necessary

We will not disclose information if it:

- Might cause serious harm to the physical or mental health of the pupil or another individual
- Would reveal that the child is at risk of abuse, where the disclosure of that information would not be in the child's best interests
- Is contained in adoption or parental order records
- Is given to a court in proceedings concerning the child

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

A request will be deemed to be unfounded or excessive if it is repetitive, or asks for further copies of the same information.
When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO.

9.3 Other data protection rights of the individual
In addition to the right to make a subject access request (see above), and to receive information when we are collecting their data about how we use and process it (see section 7), individuals also have the right to:

- Withdraw their consent to processing at any time
- Ask us to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Challenge processing which has been justified on the basis of public interest
- Request a copy of agreements under which their personal data is transferred outside of the European Economic Area
- Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them)
- Prevent processing that is likely to cause damage or distress
- Be notified of a data breach in certain circumstances
- Make a complaint to the ICO
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)

Individuals should submit any request to exercise these rights to the DPO. If staff receive such a request, they must immediately forward it to the Headteacher, Deputy Headteacher or Business Manager, who then pass it to the DPO.

Subject access requests for all or part of the pupil's educational record will be provided within 15 school days. The table below summarises the charges that apply.

NUMBER OF PAGES OF INFORMATION TO BE SUPPLIED	MAXIMUM FEE (£)
1-19	1.00
20-29	2.00
30-39	3.00
40-49	4.00
50-59	5.00
60-69	6.00
70-79	7.00
80-89	8.00
90-99	9.00
100-149	10.00
150-199	15.00
200-249	20.00

250-299	25.00
300-349	30.00
350-399	35.00
400-449	40.00
450-499	45.00
500+	50.00

If a subject access request does not relate to the educational record, we will respond within 40 calendar days. The maximum charge that will apply is £10.00.

10. CCTV

We use CCTV in various locations around the school site to ensure it remains safe. We will adhere to the ICO's code of practice for the use of CCTV.
We do not need to ask individuals' permission to use CCTV, but we make it clear where individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use.
Any enquiries about the CCTV system should be directed to the Headteacher.
Please refer to out Trust CCTV policy

11. PHOTOGRAPHS AND VIDEOS

As part of our school activities, we may take photographs and record images of individuals within our school.
We will obtain written consent from parents/carers for photographs and videos to be taken of their child for communication, marketing and promotional materials. We will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil. Where we need parental consent, we will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil. Where we don't need parental consent, we will clearly explain to the pupil how the photograph and/or video will be used.
Uses may include:

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

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not distribute it further.
When using photographs and videos in this way we will not accompany them with any other personal information about the child, to ensure they cannot be identified.
See our Child Protection and safeguarding policies for more information on our use of photographs and videos.

12. STORAGE OF RECORDS

- Paper-based records and portable electronic devices, such as laptops and hard drives, that contain personal information are kept under lock and key when not in use
- Papers containing confidential personal information should not be left on office and classroom desks, on staffroom tables or pinned to noticeboards where there is general access
- Where personal information needs to be taken off site (in paper or electronic form), staff must be aware of and comply with all elements of this policy with regard to such events. It will be rare that paper documents would need to be taken away as the vast majority of information is now available in electronic format.
- Passwords that are at least 8 characters long containing letters and numbers are used to access school computers, laptops and other electronic devices. Staff and pupils are reminded to change their passwords at regular intervals
- Encryption software is used to protect all portable devices and removable media, such as laptops.
- Staff and trustees and governors are not permitted to use USB pen drives etc. for storing and transport of information. They are permitted to use the One Drive or Drop Box. Both of these companies comply with the correct legislation in relation to storage and protection of information in relation to the law.
- Staff, pupils, trustees or governors who store personal information on their personal devices are expected to follow the same security procedures for school-owned equipment

13. DATA PROTECTION BY DESIGN AND DEFAULT

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

- Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge
- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law
- Completing privacy impact assessments where the school's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies
- Integrating data protection into internal documents including this policy, any related policies and privacy notices
- Regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters; we will also keep a record of attendance
- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant
- Maintaining records of our processing activities, including:

- For the benefit of data subjects, making available the name and contact details of our school and DPO and all information we are required to share about how we use and process their personal data (via our privacy notices)
- For all personal data that we hold, maintaining an internal record of the type of data, data subject, how and why we are using the data, any third-party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure

14. DATA SECURITY AND DISPOSAL OF RECORDS

We will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage.
In particular:

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data are kept under lock and key when not in use
- Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, pinned to notice/display boards, or left anywhere else where there is general access
- Where personal information needs to be taken off site, staff must sign it in and out from the school office
- Passwords that are at least 8 characters long containing letters and numbers are used to access school computers, laptops and other electronic devices. Staff and pupils are reminded to change their passwords at regular intervals
- Encryption software is used to protect all portable devices and removable media, such as laptops
- Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected, such as password protection.

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it.
For example, we will shred or incinerate paper-based records, and overwrite or delete electronic files. We may also use a third party to safely dispose of records on the school's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

Please refer to our Record Management Policy for more information.

15. PERSONAL DATA BREACHES

The school will make all reasonable endeavours to ensure that there are no personal data breaches.
In the unlikely event of a suspected data breach, we will follow the procedure set out in appendix 1.

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

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

16. TRAINING

Our staff and trustees are provided with data protection training as part of their induction process.
Data protection will also form part of continuing professional development, where changes to legislation or the school's processes make it necessary, such as the implementation of the General Data Protection Regulation Act

17. MONITORING ARRANGEMENTS

The Headteacher is responsible for monitoring and reviewing this policy.
The leadership team checks that the school complies with this policy by, among other things, reviewing school records at regular intervals.
This document will be reviewed when the General Data Protection Regulation comes into force, and then **every 2 years**.
At every review, the policy will be shared with the trust/governing board.

18.LINKS WITH OTHER POLICIES

This data protection policy is linked to the:
Freedom of information publication scheme.
CCTV policy
Privacy Notice Policy.

Appendix 1: Personal data breach procedure

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

On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the DPO

The DPO will investigate the report, and determine whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidentally or unlawfully:

- Lost
- Stolen
- Destroyed
- Altered
- Disclosed or made available where it should not have been
- Made available to unauthorised people

The DPO will alert the executive head, headteacher and the chair of trustees

The DPO will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary (actions relevant to specific data types are set out at the end of this procedure)

The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen

The DPO will work out whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the DPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:

- Loss of control over their data
- Discrimination
- Identify theft or fraud
- Financial loss
- Unauthorised reversal of pseudonymization (for example, key-coding)
- Damage to reputation
- Loss of confidentiality
- Any other significant economic or social disadvantage to the individual(s) concerned

If it's likely that there will be a risk to people's rights and freedoms, the DPO must notify the ICO.

The DPO will document the decision (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored.

Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website, or through their breach report line (0303 123 1113), within 72 hours. As required, the DPO will set out:

- A description of the nature of the personal data breach including, where possible:
    - The categories and approximate number of individuals concerned
    - The categories and approximate number of personal data records concerned
- The name and contact details of the DPO
- A description of the likely consequences of the personal data breach
- A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned

If all the above details are not yet known, the DPO will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible

The DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPO will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:

- A description, in clear and plain language, of the nature of the personal data breach
- The name and contact details of the DPO
- A description of the likely consequences of the personal data breach
- A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned

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

The DPO will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies

The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:

- Facts relating to the breach
- Effects
- Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)

Records of all breaches will be stored.

The DPO and headteacher will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible

Actions to minimise the impact of data breaches

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

If special category data is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error

Members of staff who receive personal data sent in error must alert the sender and the DPO as soon as they become aware of the error

If the sender is unavailable or cannot recall the email for any reason, the DPO will ask the ICT department to recall it

In any cases where the recall is unsuccessful, the DPO will contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way

The DPO will ensure we receive a written response from all the individuals who received the data, confirming that they have complied with this request

The DPO will carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted

Appendix 2: Data retention schedule

Management Data				
Record	**File Action**	**Minimum Retention Period**	**Statutory Provision**	**Action After Retention**
Board of Trustees – general correspondence	Close at end of current school year	Current year + 3 years		Destroy
FGB Meetings Minutes (master)	Close at end of current school year	10 years from the date of the meeting		Destroy
Senior Management Team-Meeting Minutes	Close at end of current school year	Date of meeting + 5 years		Destroy
Staff Meeting Minutes	Close at end of current school year	Normal Review		Determination on Review
School Development Plan	Retain whilst valid – close when superseded	Life of the plan + 3 years		Destroy
Curriculum Policies	Retain whilst valid – close when superseded	Until superseded		Keep 1 copy of previous policies and destroy all others

Policy Statements (Data Protection, Internet, Health & Safety, Child Protection, Equality etc.)	Retain whilst valid – close when superseded	Review regularly & retain latest version Older versions: date of expiry + 1 year		Destroy
PTA – minutes and general correspondence	Close at end of current school year	Normal Review		Determine on Review
Visitors Book	Close at end of current school year	End of current year + 1 years		Destroy
Circulars to Staff, Parents and Pupils	Close at end of current school year	End of current year + 2 years		Destroy
Comments/Complaints	Close at end of current school year	Date of resolution of complaint + 6 years		Archive
Annual Report	Issued every academic year	Date of Report + 10 years		Permanent Preservation
School Fund	Close at end of current financial year	Current financial year + 6 years		Destroy
Emergency Planning/Business Continuity Plan	Retain whilst valid – close when superseded	Until superseded		Destroy
CCTV	Overwritten automatically	30 days	Surveillance Camera Code of Practice 2021	Delete

Pupil				
Record	**File Action**	**Minimum Retention Period**	**Statutory Provision**	**Action After Retention**
Pupil file and records that contribute to the pupil record	Close when child leaves setting and either archived or sent to child's onwards destination	Primary - Retain whilst the child remains at the primary school Secondary - Date of birth of the pupil + 25 years	The Education (Pupil Information) (England) Regulations 2005 SI 2005 No. 1437 As amended by SI 2018 No 688 Limitation Act 1980 (Section 2)	
Pupil Admission Data	Close when register ceases to be used	Date of admission + 1 year	School Admissions Code Statutory guidance for admission authorities, governing bodies, local authorities, schools' adjudicators and admission appeals panels December 2014	Destroy
Proofs of address supplied by parents as part of the admissions process	Added to pupil file	Current year + 1 year		
Applications for enrolment	Close at end of school year in which application received	1 year from date of application		Destroy
Pupil Attendance Registers electronic	Close when register ceases to be used	3 years after the date	School attendance: Departmental advice for maintained schools, Academies,	Destroy

		on which the entry was made.	independent schools and local authorities 2014	
Pupil Education Records - School/Progress Reports etc.	Close when pupil leaves school	Lifetime of pupil file		Destroy
Special Education Needs files, reviews and Education, Health and Care Plan, including advice and information provided to parents regarding educational needs and accessibility strategy	Close when pupil leaves school	Date of birth of the pupil + 31 years [Education, Health and Care Plan is valid until the individual reaches the age of 25 years – the retention period adds an additional 6 years from the end of the plan in line with the Limitation Act]	Children and Family's Act 2014; Special Educational Needs and Disability Act 2001 Section 14	Destroy
Child Protection	Retain in secure, confidential storage	Until Pupil is 25 years old	"Keeping children safe in education Statutory guidance for schools and colleges"; "Working together to safeguard children. A guide to inter-agency working to safeguard and promote the welfare of children"	Destroy
Disciplinary Action (Suspension/Expulsion)/Offences – bullying	Close when pupil leaves school	Lifetime of pupil file		Destroy
Timetables + Class Groupings	Close at end of current academic year	Current School year + 1 Year		Destroy

Examination Results	Close at end of current academic year	Current School Year + 6 years		Destroy
Careers Advice	Added to pupil file	Life of pupil file		Destroy
School Meals returns	Close at end of current financial year	Current financial year + 6 years		Destroy
Free School Meal registers	Close at end of current financial year	Current financial year + 6 years		Destroy
School Trips – Financial & Administration details	Close at end of current financial year	Current financial year + 6 years		Destroy
School Trips-Attendance/Staff Supervision etc	Close on completion of trip	School may wish to complete a risk assessment to assess whether the forms are likely to be required and could decide to dispose of the consent forms at the end of the trip (or at the end of the academic year).		Destroy
Reports of Stolen/Damaged Items	Close at end of current academic year	7 years		Destroy
Medical Records – records of pupils with medical conditions and details	Close when pupil leaves school	Until pupil is 22 years old or in the case of a Special		Destroy

for the administration of drugs when necessary.		Needs pupil, until 25 years old		
Personnel				
Record	**File Action**	**Minimum Retention Period**	**Statutory Provision**	**Action After Retention**
Staff Personnel Records (including recruitment, interview notes, appointment details, training, staff development etc.)	Close when member of staff leaves school	During validity + 6 years after leaving employment	Limitation Act 1980 (Section 2)	Destroy
Staff Salary Records	Close at end of current financial year	Last Day of Employment + 85 Years		Archive for Pension purposes
Staff Sickness Records (copies of Medical Certs)	Close at end of current academic year	Current academic year + 6 years		Destroy
Substitute Teacher Records	Close at end of current academic year	Current academic year + 6 years		Destroy
Substitute Staff Records-non teaching (cover for nursery assistants)	Close at end of current academic year	Current academic year + 6 years		Destroy
Student Records-non teaching (e.g. nursery assistant students & pupils from schools on work experience)	Close at end of current academic year	Current academic year + 6 years		Destroy

Student Teachers on Teaching Practice – student teacher progress	Close at end of current academic year	Current academic year + 6 years		Destroy
Procedures for Induction of Staff		Until superseded		Destroy
Staff/Teacher's Attendance Records	Close after leaving employment	7 years after leaving		Destroy
Staff Performance Review	Close at end of review period covered	During validity		Destroy
Records relating to any allegation of a child protection nature against a member of staff		Until the person's normal retirement age or 10 years from the date of the allegation (whichever is the longer) then REVIEW.	"Keeping children safe in education Statutory guidance for schools and colleges September 2018"; "Working together to safeguard children. A guide to inter-agency working to safe- guard and promote the welfare of children 2018"	
Finance				
Record	**File Action**	**Minimum Retention Period**	**Statutory Provision**	**Action After Retention**
Annual Budget	Close at end of current financial year	Current financial year + 6 years		Destroy
Budget Monitoring	Close at end of current financial year	Current financial year + 3 years		Destroy

Annual Statement of Accounts (Outturn Statement)	Close at end of current financial year	Current financial year + 6 years		Archive
Order Books, Invoices, Bank Records, Cash Books, Till Rolls, Lodgment books etc.	Close at end of current financial year	Current financial year + 6 years		Destroy
Postage Book	Close at end of current financial year	Current financial year + 6 years		Destroy
Purchasing – Tender Information & Prices		Until superseded		Destroy contract schedules when they expire.
Audit Reports	Close at end of current financial year	Current financial year + 6 years		Destroy
All records relating to the management of contracts under signature		Last payment on the contract + 6 years	Limitation Act 1980	Destroy contract when they expire.
Health and Safety				
Record	**File Action**	**Minimum Retention Period**		**Action After Retention**

Accident / Incident Book	Close after last entry in book	Date of closure + 12 years	Social Security (Claims and Payments) Regulations 1979 Regulation	Destroy
Legal /Accident/Incident Forms		Until pupil is at least 22 years old or in the case of an adult 4 years from the date of the accident	25. Social Security Administration Act 1992 Section 8. Limitation Act 1980 Social Security (Claims and Payments) Regulations 1979. SI 1979 No 628 Social Security (Claims and Payments) Regulations SI 1987 No 1968 Revokes all but Part 1 of SI 1979 No 628 Social Security Administration Act 1992 Section 8. Social Security (Claims and Payments) Amendment (No	Destroy

			30 Regulations 1993 SI 1993 No 2113 Allows the information to be kept electronically	
Risk Assessments – work experience locations/pupils		Life of risk assessment + 3 years provided that a copy of the risk assessment is stored with the accident report if an incident has occurred		Destroy
H & S Reports		Current Year + 20 years		Destroy
Fire Procedure		Until superseded		Retain copies of earlier versions
Security System File		For the life of the system		Destroy
HS Policy Statement		Date of expiry + 1 Year		Destroy