St Laurence School

Data Protection Policy

Date of last review:	Sep 2021	**Review period:**	2 year
Date of next review:	Sep 2023	**Owner:**	LLM

Approved September 2020
Review September 2021

Contents

1. Aims

Our school aims to ensure that all personal data collected about staff, pupils, parents, governors, visitors and other individuals is collected, stored and processed in accordance with the Data Protection Legislation

This policy applies to anyone who has access to and/or is a user of school ICT systems, both in and out of the School, including staff, governors, students, volunteers, parents / carers, visitors, contractors, and other community users.

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

Commented [MK1]: I would recommend that this is a separate section called "scope".

2. Legislation and guidance

This policy meets the requirements of the Data Protection Legislation. It is based on guidance published by the Information Commissioner's Office (ICO) on the UK GDPR and the ICO's code of practice for subject access requests.

It meets the requirements of the Protection of Freedoms Act 2012 when referring to our use of biometric data.

It also reflects the ICO's code of practice for the use of surveillance cameras and personal information.

In addition, this policy complies with our funding agreement and articles of association.

3. Definitions

Commented [C2]: These terms are defined in the Data Protection Legislation. Those are the definitions that should be used.

Commented [RL3R2]: See below

Term	Definition
Personal data	any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. This may include (but is not limited to) the individual's: • Name (including initials) • Identification number • Location data • Online identifier, such as a username
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

Commented [RL4]: Definition added

	• Political opinions • Religious or philosophical beliefs • Trade union membership • Genetics • Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes • Health – physical or mental • Sex life or sexual orientation
Data Protection Legislation	All applicable Law about the processing of personal data and privacy, including: • UK GDPR • Data Protection Act 2018
Law	Any law, subordinate legislation within the meaning of section 21(1) of the Interpretation Act 1978, bye-law, enforceable right within the meaning of section 2 of the European Communities Act 1972, regulation, order, regulatory policy, mandatory guidance or code of practice, judgment of a relevant court of law, or directives or requirements with which the school is bound to comply.
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,

Commented [MK5]: Not sure this definition is necessary

I agree.

	unauthorised disclosure of, or access to personal data.

4. The data controller

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

The school is registered as a data controller with the ICO and will renew this registration annually or as otherwise legally required.

5. Roles and responsibilities

This policy covers applies to anyone who has access to and/or is a user of school ICT systems, both in and out of the School, including staff, governors, students, volunteers, parents / carers, visitors, contractors, and other community users.

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

5.1 Governing Body

The Governing Body has overall accountability 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 legislation, and developing related policies and guidelines where applicable.

The DPO will provide an annual report of his / her activities directly to the governing body and, where relevant, report to the body his / her advice and recommendations on school data protection issues.

The DPO is also the first point of contact for the ICO.

Full details of the DPO's responsibilities are set out in their job description in accordance with Article 39 UK GDPR. Our DPO is i-West and is contactable via i-west@bathnes.gov.uk

5.3 Headteacher

The headteacher acts as the representative of the data controller on a day-to-day basis and will liaise with the DPO. In the Headteacher's absence, in case of emergency, this role will be delegated to **********

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 Trust Data Protection Lead (Director of Finance and Operations) in the first instance, who will contact the Data Protection Officer (DPO iWest) 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

Commented [MK6]: I think this statement isn't necessary.

Commented [LL7R6]:

Commented [MK8]: This is repeated from the first paragraph of the policy.

Commented [MK9]: Possibly worth separating this paragraph out (i.e. as section 6) so you can include more contact information for One West (i.e. phone and address)

Commented [C10]: Does this work with 5.3 and 5.4 below?

Commented [RL11R10]: Ive suggested taking out the following as the first point of contact will be the school, whereas we are the liaison between the school/ICO.

Commented [C12]: And Governors?

Commented [MK13]: There should be more responsibilities for All Staff, e.g. familiarising themselves with the policy, please see our template for more.

- 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 Data Protection Legislation is based on data protection principles that our school must comply with.

The principles say that personal data must be:

- Processed lawfully, fairly and in a transparent manner - the school will explain to individuals why the school needs their data and why it is processing it – for example on consent forms (where consent is used as the basis for processing), and in its Privacy Notice(s). The school reviews its documentation and the basis for processing data on a regular basis
- Collected for specified, explicit and legitimate purposes – the school explains these reasons to the individuals concerned when it first collects their data. If the School wishes to use personal data for reasons other than those given when the data was first obtained, it will inform the individuals concerned before doing so, and will seek consent where necessary and appropriate unless the new purpose is compatible with that in respect of which consent was given, or there is another lawful basis for sharing the information/ The school will document the basis for processing.
- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed - the school must only process the minimum amount of personal data that is necessary in order to undertake its work
- Accurate and, where necessary, kept up to date - the school will check the details of those on its databases at appropriate intervals and maintain the databases. It will consider and respond to requests for inaccurate data to be rectified in accordance with the Data Protection Act 2018.
- Kept for no longer than is necessary for the purposes for which it is processed - We review what data we hold at appropriate intervals – for example upon the annual review of the Record of Processing Activities (or sooner if needed). When the School no longer needs the personal data it holds, it will ensure that it is deleted or anonymised in accordance with the retention schedule. We only keep personal data, include special category data in an identifiable form for as long as is necessary for the purposes for which it was collected, or where there is a legal obligation to do so;
    - We have a retention and disposal policy which governs how long all data including special category data shall be retained for. This policy is complied with and reviewed regularly;
    - Once the data is no longer needed, we delete it, securely destroy it in line with our retention and disposal policy, or render it permanently anonymous.
- Processed in a way that ensures it is appropriately secure - the school implements appropriate technical measures to ensure the security of data and systems for staff and all users. Further information can be found in Section 15 of this policy.
- Accountability principle – The School complies with its obligations under data protection laws including the UK GDPR and can demonstrate this via the measures set out in this policy, including:
    - Completing Data Protection Impact Assessments (DPIAs) where the School's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies. This largely involves special category personal data and CCTV. However, the School will liaise with the DPO who will advise on this process. Any activity involving the

Commented [MK14]: This seems to be a shorter version of our template. I think the explanations following each bullet point should not be removed.

Commented [RL15R14]: I agree, as these explanations are the implementation of the principles. These are required for an Appropriate Policy Document (APD) which is needed in law for processing special category personal data. Our template includes these so a separate APD is not needed.

I've added them back in.

processing of personal data must be registered on the Register of Processing Activity and reviewed, at the very least, annually;

- 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; the School also maintains a record of attendance;
- Regularly conducting reviews and audits to test its privacy measures and ensure compliance with relevant legislation and school policies;
- Maintaining records of its processing activities for all personal data that it holds.
- Policies related to the handling of data and associated documentation will be regularly reviewed on a rolling basis and updated in accordance with new guidance, legislation and practice. They will be publicised to staff who will be required to familiarise themselves with them;
- The Record of Processing Activities will be maintained and reviewed at least annually;
- Where any breaches of personal data have occurred, the reasons for this will be reviewed and changes made to practice and procedure as appropriate;
- Stakeholders will manage risks and compliance using the annual compliance statement provided by the Data Protection Officer and/or a Risk Register.

Commented [RL16]: Added back in from template – but please check to ensure this is what you do.

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

7. Processing personal data

Commented [MK17]: This section should also include information about Criminal Offenses (see our template).

Commented [RL18R17]: I would leave criminal data out of it, unless of course you process it?

We will only process personal data where we have one of 5 'lawful bases' (legal reasons) to do so under data protection law:

- The data needs to be processed so that the school can **fulfil a contract** with the individual, or the individual has asked the school to take specific steps before entering into a contract
- The data needs to be processed so that the school can **comply with a legal obligation**
- The data needs to be processed to ensure the **vital interests** of the individual e.g. to protect someone's life
- The data needs to be processed so that the school, as a public authority, can perform a task **in the public interest,** and carry out its official functions
- The individual (or their parent/carer when appropriate in the case of a pupil) has freely given clear **consent**

For special categories of personal data, we will also meet one of the special category conditions for processing which are set out in the Data Protection Legislation. This is because special category data is more sensitive, and so needs more protection. For example, information about an individual's:

Commented [MK19]: This is repeated below.

- race;
- ethnic origin;
- politics;
- religion;
- trade union membership;
- genetics;
- biometrics (where used for ID purposes);
- health;
- sex life; or
- sexual orientation

Commented [MK20]: This is a repetition of the definition.

In addition to the legal basis to process personal data, special categories of personal data also require an additional legal basis for processing under Article 9 of the UK GDPR. These grounds are as follows:

a. The individual has given **explicit consent** to the processing of those personal data for one or more specified purposes.

b. Processing is necessary for the purposes of carrying out the obligations and exercising specific rights under **employment, health and social security and social protection law and research**; a full list can be found in Schedule 1 Part 1 of the Data Protection Act 2018.

   Health or social care purposes includes the following purposes-

   i. Preventative or occupational medicine

   ii. The assessment of the working capacity of the employee

c. Processing is necessary to protect the **vital interests** of the individual or of another natural person where the individual is physically or legally incapable of giving consent.

d. Processing is carried out in the course of its legitimate activities with appropriate safeguards by a **foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim** and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the individuals concerned.

e. Processing relates to personal data which are **manifestly made public by the individual.**

f. Processing is necessary for the **establishment, exercise or defence of legal claims** or whenever courts are acting in their judicial capacity.

g. Processing is necessary for reasons of **substantial public interest** but must be clearly demonstrated and assessed as part of the public interest test and evidenced throughout the decision-making process.

   These grounds include the following (the full list of defined purposes may be found in Schedule 1 Part 2 of the Data Protection Act 2018):

   - Statutory and government purposes
   - Safeguarding of children or individuals at risk
   - Legal claims
   - Equality of opportunity or treatment
   - Counselling
   - Occupational pensions

h. Processing is necessary for the purposes of **preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services** on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3.

i. Processing is necessary for reasons of **public interest in the area of public health**

j. Processing is necessary for **archiving purposes in the public interest, scientific or historical research purposes or statistical purposes**.

Deciding upon the correct legal basis for processing data can be difficult and more than one ground may be applicable. We consult with the Data Protection Officer where appropriate.

We must also comply with Schedule 1 of the Data Protection Act (as well as Articles 6 and Article 9), when we are processing data where the conditions relate to employment, health and research or substantial public interest as follows:

- Schedule 1, Part 1 of the Data Protection Act 2018 which provides that processing under points (b), (h), (i) or (j) of the UK GDPR above (conditions relating to employment, health and research).
- Schedule 1, Part 2 of the Data Protection Act 2018 in respect of point (g) above (substantial public interest)

The Schedules can be found in the Data Protection 2018 and further define the grounds thereby offering further protections. This policy satisfies the requirements of the Schedule.

Our Privacy Notice, which may be found on our website, sets out the types of special category data that we process.

If we offer online services to pupils, such as classroom apps, and we intend to rely on consent as a basis for processing, we will get parental consent where the pupil is under 13 (except for online counselling and preventive services).

Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law in the form of privacy notices.

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. See section 7.1 for the legal basis

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.

Commented [MK21]: If the extended explanations of the Principles are retained, this section is unnecessary.

Commented [RL22R21]: I've added them back in so you can take this out

Commented [C23]: But paragraph 7 still applies. I suggest what follows is added as examples to paragraph 7.

Commented [RL24R23]: This section specifically talks about sharing/disclosure so I would keep it in.

Para 7 relates to the lawful basis for processing which is different

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 processing 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 UK, we will do so in accordance with the Data Protection Legislation.

9. Subject access requests and other rights of individuals

9.1 Subject access requests

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

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

Whilst Subject access requests can be submitted verbally, we will always follow up in writing, either by letter, email or fax to the DPO – to ensure we have an appropriate log of the request. The request should include:

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

If staff receive a subject access request they must immediately forward it to the DPL in the first instance.

9.2 Children and subject access requests

Personal data about a child belongs to that child, and not the child's parents or carers. For a parent or carer to make a subject access request with respect to their child, the child must either be unable to understand their rights and the implications of a subject access request, or have given their consent.

Children aged 12 and above are generally 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 not be granted without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

9.3 Responding to subject access requests

When responding to requests, we:

- Will verify the requester – which may require the individual to provide 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.

9.4 Other data protection rights of the individual

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

- Withdraw their consent to processing at any time
- Ask us to rectify, erase or restrict processing of their personal data, 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 UK
- 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 DPO.

10. Parental requests to see the educational record

There is no automatic parental right of access to the educational record in your setting, but you may choose to provide this.

Commented [C25]: Freedom of Information?

Commented [RL26R25]: This is a separate piece of legislation so I would not include it here. FOI allows access to school data (and not personal data).

Commented [RL27]: If you (as an academy) chose to not respond to requests under The Education (Pupil Information) (England) Regulations 2005 then I would state this in here. You may wish to soften this by including information on the annual reports that parents will receive (I assume annual reports are issued!?)

ICO Guidance: https://ico.org.uk/your-data-matters/schools/pupils-info/

11. Biometric recognition systems

Where we use pupils' biometric data as part of an automated biometric recognition system (for example, pupils use finger prints to receive school dinners instead of paying with cash), we will comply with the requirements of the Protection of Freedoms Act 2012.

Parents/carers will be notified before any biometric recognition system is put in place or before their child first takes part in it. The school will get written consent from at least one parent or carer before we take any biometric data from their child and first process it.

Parents/carers and pupils have the right to choose not to use the school's biometric system(s). We will provide alternative means of accessing the relevant services for those pupils. For example, pupils can pay for school dinners by using a pin number instead of fingerprint recognition if they wish

Parents/carers and pupils can object to participation in the school's biometric recognition system(s), or withdraw consent, at any time, and we will make sure that any relevant data already captured is deleted.

As required by law, if a pupil refuses to participate in, or continue to participate in, the processing of their biometric data, we will not process that data irrespective of any consent given by the pupil's parent(s)/carer(s).

Where staff members or other adults use the school's biometric system(s), we will also obtain their consent before they first take part in it and provide alternative means of accessing the relevant service if they object. Staff and other adults can also withdraw consent at any time, and the school will delete any relevant data already captured.

12. 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. DPIAs are completed for any changes to or additional CCTV.

This is explained in more detail in our CCTV Policy.

Any enquiries about the CCTV system should be directed to Lorna Lumb Director of Finance and Operations

13. 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, or pupils aged 16 and over, for photographs and videos to be taken of pupils for communication, marketing and promotional materials.

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 such as the school photographer, newspapers, campaigns
- Online on our school website or social media pages

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

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

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

14. Data protection by design and default

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

- Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge
- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law (see section 6)
- Completing Data Protection Impact Assessments where the school's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on this process)
- Integrating data protection into internal documents including this policy, any related policies and privacy notices
- Regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters; we will also keep a record of attendance
- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant
- Maintaining records of our processing activities, including:
    - For the benefit of data subjects, making available the name and contact details of our school and DPO and all information we are required to share about how we use and process their personal data (via our privacy notices)
    - For all personal data that we hold, maintaining an internal record of the type of data, data subject, how and why we are using the data, any third-party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure

15. Data security and storage of records

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 and USB devices
- Staff, pupils or governors who store personal information on their personal devices are expected to follow the same security procedures as for school-owned equipment (see our ICT and eSafety Policy 2018)

Commented [RL28]: Does this happen in practice??

- Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected (see section 8).

16. Bring Your Own Device (BYOD)

Student Owned Devices

The School has implemented a scheme whereby students may undertake study using their own, school-approved, mobile devices.

- Such devices remain the property of the student, and they, together with any other personal devices using the school system, are restricted through the implementation of technical solutions that provide appropriate levels of network access;
- Personal devices are brought into the School entirely at the risk of the owner;
- The School accepts no responsibility or liability in respect of lost, stolen or damaged devices while at school or in use on activities organised or undertaken by the School;
- The School recommends insurance is purchased to cover that device whilst out of the home;
- The School accepts no responsibility for the day to day maintenance or upkeep of a user's personal device, nor for any malfunction of a device due to changes made to the device while on the School network or whilst resolving any connectivity issues;
- The School recommends that all devices are made easily identifiable and have a protective case as the devices are moved around the School
- Pass-codes or PINs must be set on personal devices to aid security;
- Users are expected to act responsibly, safely and respectfully in line with current Acceptable Use Agreements;
- Devices may not be used in public or mock examinations;

Staff Owned Devices

- Staff must not use their own devices to take images of students.
- Only school equipment may be used and images must be deleted as soon as they are no longer required, saved securely on the school system and deleted in accordance with the retention policy.
- Staff should not save the personal numbers of students to their devices, and should use trip phones where appropriate
- Pass-codes or PINs must be set on personal devices to aid security; and where possible encryption applied to the device.
- Users are expected to act responsibly, safely and respectfully in line with current Acceptable Use Agreements;
- Users must log out of school programmes and applications when they are not in use;
- The device must have the latest updates applied;
- Passwords must not be saved, for example to the browser history;
- Users must not download data locally to the device (e.g. email attachments)

17. Disposal of records

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it.

For example, we will shred or incinerate paper-based records, and overwrite or delete electronic files. We may also use a third party to safely dispose of records on the school's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

Third Party Data Processors will be asked to either return to us (in a usable format) or dispose of securely all data when the data subject leaves our organisation.

18. 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

19. Training

All staff and governors are provided with data protection training as part of their induction process.

Data protection will also form part of continuing professional development, where changes to legislation, guidance or the school's processes make it necessary.

20. Monitoring arrangements

The DPO is responsible for monitoring and reviewing this policy.

This policy will be reviewed and updated if necessary including when there are any changes to legislation. Otherwise, or from then on, this policy will be reviewed **every 1 year** and shared with the full governing board.

21. Links with other policies

This data protection policy is linked to our:

ICT Policy

Data Retentions and Records Policy

Data Breach Policy

CCTV Policy

Child Protection 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 Data Protection Lead (DPL) (Director of Finance and Operations)
- The DPL will investigate the report, and determine whether a breach has occurred. To decide, the DPL 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 DPL will then alert the Data Protection Officer, head teacher and the chair of governors
- The DPL 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 advise whether the breach should be reported to the ICO. This must be judged on a case-by-case basis. To decide, the DPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:
    - Loss of control over their data
    - Discrimination
    - Identify theft or fraud
    - Financial loss
    - Unauthorised reversal of pseudonymisation (for example, key-coding)
    - Damage to reputation
    - Loss of confidentiality
    - Any other significant economic or social disadvantage to the individual(s) concerned

  If it's likely that there will be a risk to people's rights and freedoms, the DPO must notify the ICO.
- The DPO will document the decision (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored with the DPL on the schools computer system.
- Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website within 72 hours. As required, the DPO will set out:
    - A description of the nature of the personal data breach including, where possible:
        - The categories and approximate number of individuals concerned
        - The categories and approximate number of personal data records concerned
    - The name and contact details of the DPO

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

- If all the above details are not yet known, the DPO will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible
- The DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPO will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:
  - The name and contact details of the DPO
  - A description 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
- The DPO will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies
- The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:
  - Facts and cause
  - Effects
  - Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)

  Records of all breaches will be stored by the DPL on the school's computer systems

  The DPL, DPO and head teacher 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.

Actions to be taken for Sensitive information being disclosed via email (including safeguarding records)

- If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error
- Members of staff who receive personal data sent in error must alert the sender and the DPL as soon as they become aware of the error
- If the sender is unavailable or cannot recall the email for any reason, the DPL will ask the ICT department to recall it
- In any cases where the recall is unsuccessful, the DPL 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 DPL will ensure we receive a written response from all the individuals who received the data, confirming that they have complied with this request
- The DPL 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.

Details of pupil premium interventions for named children being published on the Trust website

- If personal data is accidentally made available through public websites, the owner of the webpage must take immediate steps to ensure the data is removed by contacting the website owner or administrator
- The member of staff aware of the breach must alert the DPL as soon as they become aware of it
- The DPL will carry out an internet search to check that the information has not been further disseminated on the internet; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted

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

- All papers circulated to trustees and governors will be checked by the writer to ensure that no personal data or special category data is included in the papers
- If personal ore special category data is shared with governors, the trustee/ governor/ member of staff who becomes aware of the data breach must alert the DPL as soon as they become aware of it
- The DPL must contact all recipients of the information and ask them to delete the information and not share, publish, save or replicate it in any way
- The DPL will ensure we receive a written response from all the individuals who received the data, confirming that they have complied with this request
- The DPL will ask the writer of the papers to re-issue them with the personal data or special category data removed.

A Trust laptop or USB containing non-encrypted sensitive personal data being lost, stolen or hacked

- The member of staff aware of the breach must alert the DPL as soon as they become aware of it
- The DPL must alert the police of the loss if appropriate and take all possible steps available to them to retrieve the data.
- The DPL must make the owner of the personal data aware of the loss of the data.
- The DPL will carry out an internet search to check that the information has not been disseminated on the internet; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted.

The above is not an exhaustive list of potential breaches and each breach must be reported and action taken to reduce the impact of the breach.

END