Data Protection Policy

and

Freedom of Information Publication

Date: September 2025
Review date: September 2026
Approved by Advisory Board: October 2025

Linked with other policies:

- Safeguarding incorporating child Protection Policy
- ICT and Internet Acceptable Use Policy
- Privacy Policy
- Staff code of conduct
- Staff Handbook
- Workforce Privacy Policy

Signed:

Registered address: All Saints School (Lessingham) Limited. Company no: 10323174
Rookery Farm, Reynolds Lane, Potter Heigham, Great Yarmouth NR29 5LY

Version Control

Version	Date of review/ change(s)	Page and paragraphs affected	Summary of update
V1	Sept 2021	P12-13	Added: Freedom of Information Publication Scheme
V2	Sept 2022	Title page	Freedom of Information Publication added to policy title
		Title page	Expanded list of related policies
		P4	[Advisory Board] 'members' added
		P4 point 5.3	'Headteacher' changed to School Secretary ("representative of the data controller")
		P5 point 5.4 All Staff Bullet point 3	Added: 'representative of the data controller or" [the DPO]
	Feb 2023	Appendix 3	Amendment to staff file retention period
V3	Sept 2023	P4	Katy Millage removed as DPO
		P4 5.2	Details added of the out-sourced DPO service and the role of the school's Representative of the DPO
		P5 5.4	Added School Secretary as Representative of the DPO
		P8 point 9.4	Process for exercising the data protection rights of the individual
		P9 point 13	Added [appointing]/**outsourcing**
		P10 point 15 Disposal of Records	Addition of Destruction Log process
		Throughout, where applicable	Added 'Representative of the [DPO]'
	Nov 2023	Appendix 8	Appendix 8 removed re. 'Track and Trace'. Subsequent appendix numbers changed.
	May 2024	Appendix 9	Appendix 9 removed re. Covid testing. Subsequent appendix changed to #8
V4	Sept 2024	P5 7.1	Data collected/processed for public health purposes (public interest)
		P7 9.1 SARs	Added "manifestly unfounded or excessive or an individual requests further copies of their data following a request* **from ICO guidance*"
		P10 Point 14	Bullet points 1 & 2 clarified: • Portable electronic devices, such as laptops and hard drives, are encrypted and password protected • Paper-based records (such as parent/carer contact details) are taken off-site for trips and visits; these are held by the Trip Leader who maintains their security, and shredded immediately on return to the school. Bullet point 6: added 'on laptops/devices provided by the school only' Bullet point 7: 'removable devices' and 'USB sticks' deleted [as these are banned in school] Bullet point 8: 'e-safety policy' changed to Online Safety policy
		P14 + P29	Pupil Asset changed to Arbor
	Feb 25	Appendix 2	Retention of student records now DOB +31 years (from 25 yrs) Attendance records to be kept for 6 years (from 3 years)
		Appendix 3 – staff records	Addition to 'Records relating to the appointment of a new Headteacher '
		Appendix 7 – other records	– Confidentiality Agreements completed by ALL visitors to school – Vehicle in/out log – Cleaning contractors sign-in sheets
V5	Sept 25	Appendix 3 – staff records	Retention of Right to Work Evidence in UK Evidence changed to 6 years from date of leaving, in line with all other staff records
		P7	Representative of the Data Protection Officer

1. Aims

All Saints School aims to ensure that all personal data collected about staff, students, parents, the Advisory Board, 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 personal data, regardless of whether it is in paper or electronic format.

2. Legislation and guidance

This policy meets the requirements of the UK GDPR and the expected provisions of the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the GDPR and the ICO's code of practice for subject access requests.

In addition, this policy complies with regulation 5 of the Education (Student Information) (England) Regulations 2005, which gives parents the right of access to their child's educational record.

3. Definitions

Term	Definition
Personal data	Any information relating to an identified, or identifiable, individual. This may include the individual's: • Name (including initials) • Identification number • 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 • Health – physical or mental • Sex life or sexual orientation
Processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.
Data subject	The identified or identifiable individual whose personal data is held or processed.

Data controller	A person or organisation that determines the purposes and the means of processing of personal data.
Data processor	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

4. The data controller

The school processes personal data relating to parents, students, staff, Advisory Board members, visitors and others, and, therefore, is a data controller.
The school is registered as data controllers with the ICO and will renew this registration annually or as otherwise legally required.

5. Roles and responsibilities

This policy applies to **all staff** employed by All Saints 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 The Directors

The Directors have overall responsibility for ensuring that our school complies with all relevant data protection obligations.

5.2 Data protection officer (DPO) and Representative of the DPO

All Saints School have bought into the services of an external DPO, Data Protection Education https://dataprotection.education/what-we-do. This organisation performs all the mandatory responsibilities of the DPO assisting with data protection compliance, UK GDPR accountability and the prioritisation and management of risk.

The Representative of the DPO in school is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable. He/she is the first point of contact for individuals whose data the school processes and acts as the main point of contact with the DPO.
He/she will provide a report of activities directly to the Headteacher and Advisory Board and, where relevant, report his/her advice and recommendations on school data protection issues.

Full details of the Representative of the DPO's responsibilities are set out in their job description.

5.3 School Secretary

The School Secretary acts as the representative of the data controller on a day-to-day basis. This is Tracey Buchan who is contactable at admin@allsaintslessingham.co.uk

5.4 All staff

Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy

- Informing their school of any changes to their personal data, such as a change of address
- Contacting the School Secretary, who is the representative of the data controller and the Representative of the DPO in the following circumstances:
    - If they have 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
    - If they are engaging in a new activity that may affect the privacy rights of individuals
    - If they need help with any contracts or sharing personal data with third parties.

6. Data protection principles

The UK GDPR is based on data protection principles with which our school must comply.
The principles say that personal data must be:

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed
- Accurate and, where necessary, kept up to date
- Kept for no longer than is necessary for the purposes for which it is processed
- Processed in a way that ensures it is appropriately secure.

This policy sets out how the schools aim 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 data needs to be processed so that the school can **fulfil a contract** with the individual, or the individual has asked the school to take specific steps before entering into a contract.
- The data needs to be processed so that the school can **comply with a legal obligation.**
- The data needs to be processed to ensure the **vital interests** of the individual e.g. to protect someone's life.
- The data needs to be processed so that the school, as a public authority, can perform a task **in the public interest,** and carry out its official functions.
- The data needs to be processed for the **legitimate interests** of the school or a third party (provided the individual's rights and freedoms are not overridden).
- The individual (or their parent/carer when appropriate in the case of a student) has freely given clear **consent.**
- Data collected and processed for public health purposes is done so under the UK GDPR Article 9(2)(i) "processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health..." and Recital 54 which includes: "The processing of special categories of personal data may be necessary for reasons of public interest in the areas of public health without consent of the data subject."

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.
If we offer online services to students, such as classroom apps, and we intend to rely on consent as a basis for processing, we will get parental consent where the student 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.

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 Management of Student Records, and Retention of Student Records and other student-related information guidelines in Appendix 2.

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 student 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 students – 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 and National Insurance 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 students 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.

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

Subject access requests should include:

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

Any individual wishing to exercise the right should apply in writing to the Representative of the Data Protection Officer via the school's address.
Any member of staff receiving an SAR should forward this to the school's Representative of the Data Protection Officer. The school reserves the right to charge a fee for data subject access requests (currently £25), if it is manifestly unfounded or excessive or an individual requests further copies of their data following a request*
**from ICO guidance*

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.
Juniors
Children below the age of 13 are generally not regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, some subject access requests from parents or carers of students at our school may be granted without the express permission of the student. This is not a rule and a student's ability to understand their rights will always be judged on a case-by-case basis.
Seniors
Children aged 13 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 students at our school may not be granted without the express permission of the student. This is not a rule and a student's ability to understand their rights will always be judged on a case-by-case basis.

9.3 Responding to subject access requests

When responding to requests, we:

- May ask the individual to provide 2 forms of identification
- May contact the individual via phone to confirm the request was made
- Will respond without delay and within 15 working days of receipt of the request
- 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
- The school reserves the right to charge a fee for data subject access requests (currently £25).

We will not disclose information if it:

- Might cause serious harm to the physical or mental health of the student 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 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 Representative of the DPO, which must be acted on immediately.

10. Parental requests to see the educational record

In independent schools there is no automatic parental right of access to the educational record, but we choose to provide this.

Parents, or those with parental responsibility, have a right to free access to their child's educational record (which includes most information about a student) within 15 school days of receipt of a written request. The schools may levy a charge for providing copies of information.

11. Biometric recognition systems

At present biometric data in not used or stored for All Saints School. Should this change and a biometric system be introduced this policy will be updated.

12. Photographs and videos

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

Students below the Age of 12

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 student.

Students above the age of 12

Where we don't need parental consent, we will clearly explain to the student 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 personal information about the child, to ensure they cannot be identified.

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/outsourcing 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 privacy impact assessments where the school's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on this process)
- Integrating data protection into internal documents including this policy, any related policies and privacy notices
- 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 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:

- Portable electronic devices, such as laptops and hard drives, are encrypted and password protected
- Paper-based records (such as parent/carer contact details) are taken off-site for trips and visits; these are held by the Trip Leader who maintains their security and shredded immediately on return to the school.
- Paper-based records 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 accessed off site, staff do so on the Arbor MIS.
- All staff have access to this via logins which can therefore be accessed at home - using **laptops/devices provided by the school only.** All staff are bound by the Confidential Information and Data Protection section in their contracts. Any printed material used at home, must be kept in a locked container and then brought to school for shredding.
- 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 students are reminded to change their passwords at regular intervals.
  Encryption software is used to protect all portable devices, such as laptops
  Staff or students who store personal information on their personal devices are expected to follow the same security procedures as for school-owned equipment; see our Online Safety policy
- Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected (see section 8).

15. 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. See Appendices 2-7.
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. Disposal of all records (paper-based or electronic) are recorded on a Destruction Log, managed by the Representative of the DPO/School Secretary.

16. Personal data breaches

All Saints 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 students eligible for the student premium
- Safeguarding information being made available to an unauthorised person
- The theft of a school laptop containing non-encrypted personal data about students.

17. Training

All staff and Advisory Board members 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.

18. Monitoring arrangements

The Headteacher and Representative of the DPO are responsible for monitoring and reviewing this policy.

This policy will be reviewed and updated every two years or if there are any changes made to the current law.

19. Links with other policies

This data protection policy is linked to our:

- Safeguarding incorporating child Protection Policy
- ICT and Internet Acceptable Use Policy
- Privacy Policy
- Staff code of conduct
- Staff Handbook
- Workforce Privacy Policy

Freedom of Information Publication Scheme

Publication scheme on information available under the freedom of information act 2000
The Directorship is responsible for maintenance of this scheme.

1. **Introduction: What A Publication Scheme Is And Why It Has Been Developed**
One of the aims of the Freedom of Information Act 2000 (which is referred to as FOIA in the rest of this document) is that public authorities, including schools, should be clear and proactive about the information they will make public.
To do this we must produce a publication scheme, setting out:

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

The scheme covers information already published and information, which is to be published in the future. All information in our publication scheme is either available for you on our website to download and print off or available in paper form.
Some information, which we hold, may not be made public, for example personal information.
This publication scheme conforms to the model scheme for schools approved by the Information Commissioner.

2. **Aims and Objectives**

- Effective Learning: To provide effective learning experiences appropriate to the individual and to enable all individuals to fulfil their potential.
- Secure Environment: To provide a secure and caring environment for all the students.
- Work Attitudes: To encourage the students to develop enthusiasm, self-confidence, a spirit of enquiry, a pride in their work and the ability to work with others.
- Parental Involvement: To foster a sense of partnership between home and school so that parents will feel committed and involved in the life of the school.
- Respect: To promote self-respect and respect for other people, regardless of Age, Disability, Gender reassignment, Marriage and civil partnership, Pregnancy and maternity, Race, Religion or belief, Sex, Sexual orientation. (In Alphabetical order)
- Broad and Balanced Curriculum: To help students acquire a range of skills, knowledge and understanding that is broad and balanced in nature and relevant to their personal growth and to their adult life and to prepare them for life in the 21st century.
- Community Awareness: To increase students' awareness of their role and responsibilities in the community and to develop constructive links with the community.
- Progression through Education: To facilitate the students' progress between nursery, primary and secondary phases.

This publication scheme is a means of showing how we are pursuing these aims.

3. Categories of Information Published
The publication scheme guides you to information, which we currently publish, are available on request subject to safeguards regarding confidentiality or which we will publish in the future.

- **School Prospectus** - Information published in the School Prospectus
- **Directors' Documents** - Information published for and by The Directorship

- **Students and Curriculum** - Information about policies that relate to students and the school curriculum
- **School Policies and Other Information Related to the School** - Information about policies that relate to the school in general

4. **How to Obtain or Request Information**
If you require a paper version of any of the documents within this scheme, please contact the school by telephone, e-mail or letter. Contact details are set out below:
All Saints School, School Road, Lessingham, Norwich, Norfolk NR12 0DJ 01692 582083
office@allsaintsllessingham.co.uk

Please clearly mark any correspondence **"PUBLICATION SCHEME REQUEST"**

If the information you are looking for is not available via the scheme and is not on our website, you can still contact the school to ask if we have it.

5. **Paying for Information**
Information published on our website is free, although you may incur costs from your internet service provider. If you don't have internet access, you can access our website using a local library or an internet café.
Single copies of information covered by this publication are provided free unless stated otherwise in section 6. If your request means that we have to do a lot of photocopying or printing, or pay a large postage charge, or is for a priced item such as some printed publications, we will let you know the cost before fulfilling your request.

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 Representative of 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 Headteacher, Directors and the chair of the Advisory Board.
- 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 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 on the school's computer systems.
- 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 and Mrs R Smith (Director) 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 on the schools' computer system accessible by the Director, Headteacher and the DPO.
- 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 appropriate actions such as those 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.

e.g. Sensitive information being disclosed via email (including safeguarding records)

- *If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error.*
- *Members of staff who receive personal data sent in error must alert the sender and the DPO as soon as they become aware of the error.*
- *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

1. Management of student records

1.1 Student records are specific documents that are used throughout a student's time in the education system – they are passed to each school that a student attends and include all personal information relating to them, e.g. date of birth, home address, etc. as well as their progress and achievement.

1.2 The following information is stored on the front of a student record, and will be easily accessible:

- Forename and surname.

1.3 The following information is stored inside the front cover of a student record and will be easily accessible:

- Ethnic origin, religion and first language (if not English);
- Any preferred names;
- Emergency contact details and the name of the student's doctor;
- Any allergies or other medical conditions that are important to be aware of;
- Names of parents/carers, including their home address(es) and telephone number(s);
- Name of the school, admission number, the date of admission and the date of leaving, where appropriate;
- Any other agency involvement, e.g. speech and language therapist.

1.4 The following information is stored on a student record and will be easily accessible:

- Admission form;
- Details of any SEND;
- Fair processing notices – only the most recent notice will be included;
- Annual written reports to parents;
- Notes relating to major incidents and accidents involving the student;
- Any information about an Education and Healthcare Plan (EHCP) and support offered in relation to the EHCP;
- Any notes indicating that child protection disclosures and reports are held;
- Any information relating to exclusions;
- Any correspondence with parents or external agencies relating to major issues, e.g. mental health;
- Absence notes;
- Notes indicating that records of complaints made by parents or the student are held.

1.5 The following information is subject to shorter retention periods and, therefore, will be stored separately in the School Office:

- Parental and, where appropriate, student consent forms for educational visits, photographs and videos, etc;
- Correspondence with parents about minor issues, e.g. behaviour.

1.6 Hard copies of disclosures and reports relating to child protection are stored in individual files, in a securely locked filing cabinet in the Headteacher's office.

1.7 Hard copies of complaints made by parents or students are stored in a file in the locked confidential cupboard in the Headteacher's office.

1.8 Actual copies of accident and incident information are stored separately on the school's management information system and are held in line with the retention periods outlined in this Policy – a note indicating this is marked on the student's file. An additional copy may be placed in the student's file in the event of a major accident or incident.

1.9 The school will ensure that no student records are altered or amended before transferring them to the next school that the student will attend.

1.10 The only exception to the above is if any record placed on the student's file has a shorter retention period and may need to be removed. In such cases, the DPO responsible for disposing of records will remove these records.

1.11 Electronic records relating to a student's record will also be transferred to the student's next school using the School 2 School website in the form of a CTF (Common Transfer file).

1.12 If any student attends the school until statutory school leaving age, the school will keep the student's records until the student reaches the age of 25 years. These records are stored in the school's archive.

1.13 The school will, wherever possible, avoid sending a student record by post. Where a student record must be sent by post, it will be sent by registered post, with an accompanying list of the files included. The school to which it is sent is required to sign a copy of the list to indicate it has received the files and return this to the school.

2. Retention of student records and other student-related information

2.1 The table below outlines the school's retention periods for individual student records and the action that will be taken after the retention period, in line with any requirements.

2.2 Electronic copies of any information and files will be destroyed in line with the retention periods below.

Type of file	Retention period	Action taken after retention period ends
Admissions		
Register of admissions	Three years after the date on which the entry was made	Information is reviewed and the register may be kept permanently.
Students' educational records		
Primary Schools only – Students' educational records	Whilst the student remains at the school	Transferred to the next destination – if this is an independent school, homeschooling or outside of the UK, the file will be kept by the LA and retained for the statutory period.
Secondary Schools only –	31 years after the student's date of birth	Securely disposed of – cross shredded

Students' educational records – including ICT Acceptable Use of the Internet, Student Code of Conduct		
Public examination results	Added to the student's record	Securely disposed of – cross shredded
Internal examination results	Added to the student's record	Securely disposed of – cross shredded
Child Protection information held on student's record	Stored in a sealed envelope for the same length of time as the student's record	Securely disposed of – cross shredded.
Child Protection records held in a separate file	31 years after the student's date of birth	Securely disposed of – cross shredded.
Attendance		
Attendance registers	Last date of entry on to the register, plus six years	Securely disposed of – cross shredded.
Letters authorising absence	Current academic year, plus two years	Securely disposed of – cross shredded.
SEND		
SEND files, reviews and individual education plans	31 years after the student's date of birth (as stated on the student's record)	Information is reviewed and the file may be kept for longer than necessary if it is required for the school to defend themselves in a 'failure to provide sufficient education' case. Securely disposed of – cross shredded
Statement of SEN maintained under Section 324 of the Education Act 1996 or an EHCP maintained under Section 37 of the Children and Families Act 2014 (and any amendments to the statement or plan)	31 years after the student's date of birth (as stated on the student's record)	Securely disposed of, unless it is subject to a legal hold.
Information and advice provided to parents regarding SEND	31 years after the student's date of birth (as stated on the student's record)	Securely disposed of, unless it is subject to a legal hold.
Accessibility strategy	31 years after the student's date of birth (as stated on the student's record)	Securely disposed of, unless it is subject to a legal hold.
Curriculum management		
SATs results	31 years after the student's date of birth (as stated on the student's record)	Securely disposed of.

Examination papers	Until the appeals/validation process has been completed	Securely disposed of.
Published Admission Number (PAN) Reports	Current academic year, plus six years	Securely disposed of.
Value added and contextual data	Current academic year, plus six years	Securely disposed of.
Self-evaluation forms	Current academic year, plus six years	Securely disposed of.
Students' work	Returned to students at the end of the academic year, or retained for the current academic year, plus one year	Securely disposed of.
Extra-curricular activities		
Parental consent forms for school trips where no major incident occurred	Until the conclusion of the trip	Securely disposed of.
Parental consent forms for school trips where a major incident occurred This defined through Norfolk County Council's Evolve procedures.	31 years after the student's date of birth on the student's record (permission slips of all students on the trip will also be held to show that the rules had been followed for all students)	Securely disposed of.

Appendix 3. Retention of staff records

3.1 The table below outlines the school's retention period for staff records and the action that will be taken after the retention period, in line with any requirements.

3.2 Electronic copies of any information and files will also be destroyed in line with the retention periods below.

Type of file	Retention period	Action taken after retention period ends
Operational		
Staff members' personal files	Scanned copies: Termination of employment, plus six years. Paper copies: securely archived, held for 6 months	Deleted from SLT Drive Securely disposed of.
Annual appraisal and assessment records	Current academic year, plus five years	Securely disposed of.
Recruitment		
Records relating to the appointment of a new Headteacher	Date of leaving plus six years except in cases of negligence or claims of child abuse then at least 10 years from the date of the allegation - (school review).	Securely disposed of.
Records relating to the appointment of new members of staff (unsuccessful candidates)	Date of interview plus six months	Securely disposed of.
Records relating to the appointment of new members of staff (successful candidates)	Relevant information added to the member of staff's personal file and other information retained for six years after leaving	Securely disposed of.
Proof of identity as part of the enhanced DBS check	Held on staff file for duration of employment plus retention period	Reviewed and a note kept of what was seen and what has been checked – if it is necessary to keep a copy this will be placed on the staff member's personal file, if not, it will be securely disposed of.
Evidence of right to work in the UK	Added to staff personal file or, if kept separately, termination of employment, plus six years	Securely disposed of.

Disciplinary and grievance procedures		
Child protection allegations, including where the allegation is unproven	Added to staff personal file, and until the individual's normal retirement age, or ten years from the date of the allegation – whichever is longer. If allegations are malicious, they are removed from personal files.	Reviewed and securely disposed of – shredded.
Oral warnings	Date of warning, plus six months.	Securely disposed of – if placed on personnel file, removed from file.
Written warning – Level 1	Date of warning, plus six months	Securely disposed of – if placed on personal file, removed from file.
Written warning – Level 2	Date of warning, plus 12 months	Securely disposed of – if placed on personal file, removed from file.
Final warning	Date of warning, plus 18 months	Securely disposed of – if placed on personal file, removed from file.
Records relating to unproven incidents	Conclusion of the case, unless the incident is child protection related and is disposed of, as above.	Securely disposed of.

Securely disposed of means cross shredding

Appendix 4

4. Retention of senior leadership and management records

4.1 The table below outlines the school's retention periods for senior leadership and management records, and the action that will be taken after the retention period, in line with any requirements.

Electronic copies of any information and files will also be destroyed in line with the retention periods below.

Type of file	Retention period	Action taken after retention period ends
Advisory Board		
Agendas for the Advisory Board meetings	One copy alongside the original set of minutes – all others disposed of without retention	Securely disposed of.
Original, signed copies of the minutes of the Advisory Board meetings	Permanent	
Printed inspection copies of the minutes of Advisory Board meetings (all now kept electronically on the secure website, GovernorHub)	Date of meeting, plus three years	If printed, shredded if they contain any sensitive and personal information.
Reports presented to the Advisory Board	Minimum of six years, unless they refer to the individual reports – these are kept permanently.	Securely disposed of or, if they refer to individual reports, retained with the signed, original copy of minutes.
Terms of Reference	Permanent	
Business Continuity Plan and action plans created and administered by the Directors.	Duration of the action plan, plus three years	Securely disposed of.
Policy documents created and administered by the Advisory Board	Duration of the policy, plus three years	Securely disposed of.
Records relating to complaints dealt with by the Directors.	Date of the resolution of the complaint, plus a minimum of six years	Reviewed for further retention in case of contentious disputes, then securely disposed of.
Annual reports created under the requirements of The Education (Governors' Annual Reports) (England) (Amendment) Regulations 2002	Date of report, plus ten years	Securely disposed of.

Proposals concerning changing the status of the school	Date proposal accepted or declined, plus three years	Securely disposed of.
Headteacher and Senior Leadership Team (SLT)		
Minutes of SLT meetings and the meetings of other internal administrative bodies	Date of the meeting, plus three years	Reviewed and securely disposed of.
Reports created by the Headteacher or SLT	Date of the report, plus a minimum of three years	Reviewed and securely disposed of.
Records created by the Headteacher, deputy Headteacher and other members of staff with administrative responsibilities	Current academic year, plus six years	Reviewed and securely disposed of.
Correspondence created by the Headteacher, deputy Headteacher and other members of staff with administrative responsibilities	Date of correspondence, plus three years	Reviewed and securely disposed of.
Professional development plan	Duration of the plan, plus six years	Securely disposed of.
School development plan	Duration of the plan, plus three years	Securely disposed of.

Appendix 5

5. Retention of health and safety records

5.1 The table below outlines the school's retention periods for health and safety records, and the action that will be taken after the retention period, in line with any requirements.

5.2 Electronic copies of any information and files will also be destroyed in line with the retention periods below.

Type of file	Retention period	Action taken after retention period ends
Health and Safety		
Health and safety policy statements	Duration of policy, plus three years	Securely disposed of.
Transport and Vehicles Checklists	3 years; Caretaker completes and holds checklists on school G-Drive, deleted after 3 years.	Deleted from G Drive.
Health and safety risk assessments	Duration of risk assessment, plus three years	Securely disposed of.
Records relating to accidents and injuries at work	Date of incident, plus 12 years. In the case of serious accidents, a retention period of 15 years is applied	Securely disposed of.
Accident reporting – adults	Date of the incident, plus six years	Securely disposed of.
Accident reporting – students	25 years after the student's date of birth, on the student's record	Securely disposed of.
Control of substances hazardous to health	Current academic year, plus 40 years	Securely disposed of.
Information relating to areas where employees and persons are likely to come into contact with asbestos	Date of last action, plus 50 years	Securely disposed of.
Fire precautions log book	Current academic year, plus six years	Securely disposed of.

Appendix 6

6. Retention of financial records

6.1 The table below outlines the school's retention periods for financial records and the action that will be taken after the retention period, in line with any requirements.

6.2 Electronic copies of any information and files will also be destroyed in line with the retention periods below.

Type of file	Retention period	Action taken after retention period ends
Payroll pensions		
Maternity pay records	Current academic year, plus three years	Securely disposed of.
Records held under Retirement Benefit Schemes (Information Powers) Regulations 1995	Current academic year, plus six years	Securely disposed of.
Risk management and insurance		
Employer's Liability Insurance Certificate	Closure of the school, plus 50 years	Securely disposed of.
Asset management		
Inventories of furniture and equipment	Current academic year, plus six years	Securely disposed of.
Burglary, theft and vandalism report forms	Current academic year, plus six years	Securely disposed of.
Accounts and statements including budget management		
Annual accounts	Current academic year, plus six years	Disposed of against common standards.
Loans and grants managed by the school	Date of last payment, plus 12 years	Information is reviewed then securely disposed of.
All records relating to the creation and management of budgets	Duration of the budget, plus three years	Securely disposed of.
Invoices, receipts, order books, requisitions and delivery notices	Current financial year, plus six years	Securely disposed of.
Records relating to the collection and banking of monies	Current financial year, plus six years	Securely disposed of.

Records relating to the identification and collection of debt	Current financial year, plus six years	Securely disposed of.
Contract management		
All records relating to the management of contracts under the seal.	Last payment on the contract, plus 12 years	Securely disposed of.
All records relating to the management of contracts under signature	Last payment on the contract, plus six years	Securely disposed of.
All records relating to the monitoring of contracts	Current academic year, plus two years	Securely disposed of.
School fund		
Cheque books, paying in books, ledgers, invoices, receipts, bank statements and journey books	Current academic year, plus six years	Securely disposed of.
School meals		
Free school meals registers	Current academic year, plus six years	Securely disposed of.

Appendix 7

7. Retention of other school records

7.1 The table below outlines the school's retention periods for any other records held by the school, and the action that will be taken after the retention period, in line with any requirements.

7.2 Electronic copies of any information and files will also be destroyed in line with the retention periods below.

Type of file	Retention period	Action taken after retention period ends
Property management		
Title deeds of properties belonging to the school	Permanent	Transferred to new owners if the building is leased or sold.
Plans of property belonging to the school	For as long as the building belongs to the school	Transferred to new owners if the building is leased or sold
Leases of property leased by or to the school	Expiry of lease, plus six years	Securely disposed of.
Records relating to the letting of school premises	Current financial year, plus six years	Securely disposed of.
Maintenance		
All records relating to the maintenance of the school carried out by contractors	Current academic year, plus six years	Securely disposed of.
All records relating to the maintenance of the school carried out by school employees	Current academic year, plus six years	Securely disposed of.
Operational administration		
Records relating to the creation and publication of the school brochure and/or prospectus	Current academic year, plus three years	Disposed of against common standards.
Records relating to the creation and distribution of circulars to staff, parents or students	Current academic year, plus one year	Disposed of against common standards.
Newsletters and other items with short operational use	Current academic year, plus one year	Disposed of against common standards.

Visitors' books and signing-in sheets	Current academic year, plus six years	Reviewed then securely disposed of.
Records relating to the creation and management of parent/teacher associations and/or old student associations	Current academic year, plus six years	Reviewed then securely disposed of.
Confidentiality Agreements completed and signed by ALL visitors to school	5 years from issue	Shredded on site
Vehicle in/out log	1 term + following holiday period Following on from an incident, 3 years	Shredded on site
Cleaning contractors sign-in sheets	1 term + following holiday period	Shredded on site

Appendix 8: Next of Kin (NOK) data collection

We will only collect and process information from a 'nominated emergency contact or next of kin' of an employee of All Saints School.

Why we need Next of Kin information and how we use it

In the case of contact details in the event of an emergency where it is necessary to contact an employee's emergency contact or their next of kin, All Saints School has a legitimate interest in processing this personal data during the employment relationship of an employee. This allows the School to maintain accurate and up-to-date employment records and contact details.

What type of information is collected

All Saints School will collect this data from employees who have directly nominated their emergency contact and/or next of kin. We will collect the following information:

- name
- relationship to the employee
- contact number(s) – home/work/mobile as applicable

This information will be held on our secure MIS system, Arbor.

NOK contact details may be accessed by any member of staff if appropriate; reasons for this may include:

- The staff member has become unwell at work and taken to hospital
- The staff member has not reported for work. After failed attempts to contact the employee directly, an emergency contact/next of kin may be contacted.
- An emergency situation arises at the school, necessitating implementation of Lockdown or Evacuation.

How long we keep NOK information (retention period)

The School will hold an employee's contact data ONLY for the duration of their employment at All Saints School, or until they notify the School of a change in their emergency contact/next of kin.

How we protect the Information

Next of Kin contact details will be stored securely and processed strictly in accordance with UK GDPR. We have implemented generally accepted standards of technology and operational security in order to protect personal data from loss, misuse, or unauthorised alteration or destruction.