Data Protection Policy
A8

Dolphin School Trust
inc. Noah's Ark Nurseries

Reviewed by:	Lucy Price (Headteacher)
Last reviewed:	August 2025
Next review:	August 2027

Contents

1. Aims

Dolphin School and Noah's Ark Nursery Schools aim to ensure that all personal data collected about staff, pupils, parents, governors, visitors and other individuals is collected, stored and processed in accordance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018, as amended by the Data Protection and Digital Information Act 2025.

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 UK GDPR and the Data Protection Act 2018, as amended in 2025.
It is based on guidance published by the Information Commissioner's Office (ICO) and the ICO's code of practice for subject access requests.

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

3. Definitions

Personal data
Any information relating to an identified, or identifiable, individual.

Special categories of personal data
Personal data which is more sensitive and requires greater protection, including:

- Racial or ethnic origin
- Religious or philosophical beliefs
- Trade union membership
- Genetic or biometric data
- Health – physical or mental
- Sex life or sexual orientation
- Political opinions
- The commission or alleged commission of offences, court sentences or allegations under investigation

Processing
Any action performed on personal data, 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, including unauthorised loss of availability.

Automated decision-making / AI-assisted processing
Decisions made using digital tools, algorithms, or artificial intelligence which may significantly affect an individual. Schools will not make solely automated decisions about pupils or staff without meaningful human involvement.

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

5.1 Governing board

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

5.2 Privacy and Compliance Officer

The PCO is responsible for overseeing policy implementation, compliance monitoring, and staff guidance. They will provide an annual report of their activities directly to the governing board and, where relevant, report to the board their advice and recommendations on school data protection issues.
They also act as the first point of contact for individuals and the ICO.

The PCO must ensure Data Protection Impact Assessments (DPIAs) are carried out where required, including for AI/digital tools.

Our PCO is Vivienne Benson and is contactable via email at 'admissions@dolphinschool.org.uk'.

5.3 Head
The Head acts as the representative of the data controller on a day-to-day basis. They provide guidance to process Subject Access Requests and Freedom of information requests, and ensure appropriate and adequate training is available to staff.

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

6. Data protection principles

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

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

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

7. Collecting personal data

7.1 Lawfulness, fairness and transparency

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

1. 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
2. The data needs to be processed so that the school can **comply with a legal obligation**
3. The data needs to be processed to ensure the **vital interests** of the individual e.g. to protect someone's life
4. 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
5. 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)
6. 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 GDPR and Data Protection Act 2018, as amended in 2025.

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 (except for online counselling and preventative services).

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 Data Retention Schedule (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 pupil or parent/carer that puts the safety of our staff at risk
- We need to liaise with other agencies – we will seek consent as necessary before doing this
- Our suppliers or contractors need data to enable us to provide services to our staff and pupils – for example, IT companies. When doing this, we will:

- Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law
- Establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data we share
- Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us

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

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

We may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of our pupils or staff.

Where personal data is transferred outside the UK, we will ensure safeguards are in place as required by UK GDPR.

9. Subject access requests and other rights of individuals

9.1 Subject access requests

Individuals have the right to access their personal information. This includes confirmation of processing, access to data, processing purposes, categories of data, retention periods, recipients, sources, and details of any automated decision-making.

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

If staff receive a subject access request they must immediately forward it to the PCO.

9.2 Children and subject access requests

Requests must be submitted in writing. Proof of ID may be required.

In line with the Data Protection and Digital Information Act 2025:

- Searches will be reasonable and proportionate.
- The timeframe may be paused (“stop the clock”) while awaiting clarification.
- Complaints will be acknowledged within 30 days and responded to without undue delay.

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

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

9.3 Responding to subject access requests
When responding to requests, we may:

- Request proof of ID
- Confirm the request by phone
- Respond within one month, unless an extension (up to three months) is justified
- Pause the statutory timeframe paused (“stop the clock”) while awaiting clarification.

When responding to requests, we will:

- Conduct reasonable and proportionate searches and will not duplicate information already held by the requester.
- Acknowledge data protection complaints within 30 days and resolve them without undue delay.
- Provide the information free of charge

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 Freedom of Information Requests (FOI's)
The Freedom of Information Act 2000 (FOIA) provides public access to information held by schools. It does this in two ways: schools are obliged to publish certain information about their activities; and. members of the public are entitled to request information from schools.

Dolphin School will comply with Freedom of Information requests and release non personal and non confidential information held by the school, after applying any relevant exemptions to protect certain categories of data.
The Act requires that all requests must be in writing (to include letters, faxes and e-mails). Requests must state clearly what information is required and must provide the name of the person with an address for correspondence.

On receipt of a FOI request, a school must respond promptly and in any event within 20 working days.

See Freedom of Information guidance for details.
(For help and advice in responding to an FOI request, contact the schools data protection advisor)

9.5 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 PCO. If staff receive such a request, they must immediately forward it to the PCO.

10. Photographs and videos

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

We will obtain written consent from parents/carers for photographs and videos to be taken of their child for communication, marketing and promotional materials. We will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil.

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.

11. 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 PCO, 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)
- Integrating data protection into internal documents including this policy, any related policies and privacy notices
- Train 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
- Conduct 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 PCO 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
- Before introducing any AI or third-party digital tool that processes staff or pupil data, the school will complete a Data Protection Impact Assessment (DPIA) *see Appendix 3*

12. 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
- 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
- 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 Acceptable Use Policy)
- Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected (see section 8)

13. 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.

14. 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

15. 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. Training will include updated requirements for subject access requests, complaint handling, and responsible use of AI/digital tools.

16. Monitoring arrangements

The PCO is responsible for monitoring and reviewing this policy.
This policy will be reviewed **every 3 years** and shared with the full governing board.

17. Links with other policies

This data protection policy is linked to our:

- Safeguarding and Child Protection Policy
- Acceptable Use 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 PCO
- The PCO will investigate the report, and determine whether a breach has occurred. To decide, the PCO 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 PCO will alert the Headteacher and the Chair of Governors
- The PCO 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 PCO will assess the potential consequences, based on how serious they are, and how likely they are to happen
- The PCO 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 PCO 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 PCO must notify the ICO.
- The PCO 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 system.
- Where the ICO must be notified, the PCO will do this via the 'report a breach' page of the ICO website within 72 hours. As required, the PCO 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 PCO
    - 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 PCO 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 PCO expects to have further information. The PCO will submit the remaining information as soon as possible
- The PCO 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 PCO 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 PCO
    - 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 PCO 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 PCO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:
    - Facts and cause
    - Effects
    - Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)
    - Records of all breaches will be stored on the school's computer system
    - The PCO 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 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.

Appendix 2 – Data Retention Schedule

1) Child Protection Files

	Basic File Description	Data Protection Issue	Statutory Provisions	Retention Period	Action at End of Administrative Life of Record
1.1	Child protection files	Yes	Education Act 2002, s175, related guidance "Safeguarding Children in Education", September 2004. Data Protection in Schools Feb 2023 Keeping children safe in education, sections 122 and 123. The Report of the Independent Inquiry into Child Sexual Abuse (IICSA) recommendation on access to records.	Date of birth + 25 years If the record relates to child sexual abuse, retain until the individual's 75th birthday	Secure disposal
1.2	Allegation of child protection nature against a member of staff, including where the allegation is unfounded	Yes	Employment Practices Code: Supplementary Guidance 2.13.1 (Records of Disciplinary and Grievance). Education Act 2002 Guidance "Dealing with Allegations of Abuse against Teachers and Other Staff" November 2005 Keeping children safe in education. Working together to safeguard children.	Until the person's normal retirement age, or 10 years from the date of the allegation whichever is the longer	Secure disposal

2) Governors

	Basic File Description	Data Protection Issue	Statutory Provisions	Retention Period	Action at End of Administrative Life of Record
2.1	Minutes	No		Permanent	Must be available in school for 6 years from the meeting. Can then be archived/stored elsewhere.
2.2	Agendas	No		Date of meeting	Secure disposal
2.3	Reports	No	The Education (Governors' Annual Reports) (England) (Amendment) Regulations 2002. Retain as detailed in section 2 of the Limitation Act 1980.	Date of report + 10 years	Retain in school for 10 years from report date. Can consider archiving/storing anything important.
2.4	Annual parents' meeting papers	No		Date of meeting + 6 years	Retain in school for 6 years from meeting date. Can consider archiving/storing anything important.
2.5	Instruments of Government	No		Permanent	Retain in school whilst school open. Can then be archived/stored elsewhere.
2.6	Trusts and Endowments	No		Permanent	Retain in school whilst operationally required. Can then be archived/stored elsewhere.
2.7	Action plans	No		Date of action plan + 3 years	Secure disposal
2.8	Policy documents	No		Expiry of policy	Retain in school whilst policy operational (this includes if the expired policy is part of a past decision making process).

2.9	Complaints files	Yes		Date of resolution of complaint + 6 years	Review for further retention in the case of contentious disputes. Secure disposal.
2.10	Proposals for schools to become or be established as Specialist Status schools	No		Current year + 3 years	Secure disposal

3) Management

	Basic File Description	Data Protection Issue	Statutory Provisions	Retention Period	Action at End of Administrative Life of Record
3.1	Minutes of the senior management team and other internal administrative bodies	Yes		Date of meeting + 5 years	Retain in school for 5 years from meeting date. Can consider archiving/storing anything important.
3.2	Reports made by the Headteacher or senior management team	Yes		Date of report + 3 years	Retain in school for 3 years from report date. Can consider archiving/storing anything important.
3.3	Records created by Headteacher, Deputy Heads, key stage coordinators, and other members of staff with administrative responsibilities	Yes		Closure of file + 6 years	Secure disposal
3.4	Correspondence created by Headteacher, Deputy Heads,key stage coordinators and other members of staff with administrative responsibilities	No/Yes		Date of correspondence + 3 years	Secure disposal
3.5	Professional development plans	Yes		Closure + 6 years	Secure disposal
3.6	School development plans	No		Closure + 6 years	Review for further retention. Secure disposal.

3.7	Admissions to Dolphin School - if the application is successful	Yes	Data Protection in Schools June 2025 Working Together to improve school attendance 2024	Admission + 1 year	Secure disposal
3.8	Admissions to Dolphin School- if the application is unsuccessful	Yes	Data Protection in Schools June 2025, Working Together to improve school attendance 2024		Secure disposal
3.9	Secondary School acceptance information	Yes		6 years	Secure disposal
3.10	Supplementary information form including additional information such as religion, medical conditions supplied as part of the admissions process	Yes		As the corresponding admission record	Secure disposal

4) Pupils

	Basic File Description	**Data Protection Issue**	**Statutory Provisions**	**Retention Period**	**Action at End of Administrative Life of Record**
4.1	Admission registers	Yes	Data Protection in Schools June 2025, Working Together to improve school attendance 2024	Entry + 6 years	Retain in school for 7 years from entry. Can consider archiving these records if have the facility.

			Regulation 7 of the School Attendance (Pupil Registration) (England) Regulations 2024.		
4.2	Attendance registers	Yes	Data Protection in Schools June 2025, Working Together to improve school attendance 2024 Regulation 7 of the School Attendance (Pupil Registration) (England) Regulations 2024	Date of register + 6 years	Secure disposal
4.3	Pupil files	Yes		Retain for time which the pupil remains at the primary school	Transfer to the secondary school (or other primary school) when the child leaves the school.
4.4	Special Educational Needs and disabilities files, reviews and individual education, health and care plans	Yes	SEND code of practice: 0 to 25 years. Retain as detailed in section 2 of the Limitation Act 1980. Regulation 17 of The Special Educational Needs and Disability Regulations 2014.	Retain until pupil's 25th birthday if part of main pupil record. If stored separately, retain for 12 years after pupil leaves school unless linked to safeguarding, in which case retain until 25th birthday. EHC Plans to be retained for 6 years after cessation	Secure disposal, unless the document is subject to a legal hold. If the pupil leaves to go to another school, transfer the records to that school.
4.5	Correspondence relating to authorised absence and issues	Yes		Date of absence + 2 years	Secure disposal

4.6	Public Examinations	No		Year of examination + 6 years	Secure disposal
4.7	Internal examination results	Yes		Current year + 1 year	Secure disposal
4.8	Any other records created in the course of contact with pupils	Yes/No		Current year + 3 years	Review at the end of 3 years and retain with pupil file if necessary. Secure disposal
4.9	Statement maintained under the Education Act 1996 Section 324	Yes	Special Educational Needs and Disability Act 2001 Section 1	Date of birth + 30 years	Secure disposal unless legal action is pending
4.10	Proposed statement or amended statement	Yes	Special Educational Needs and Disability Act 2001 Section 1	Date of birth + 30 years	Secure disposal unless legal action is pending
4.11	Advice and information to parents regarding educational needs	Yes	Special Educational Needs and Disability Act 2001 Section 2	Closure + 12 years	Secure disposal unless legal action is pending

	Basic File Description	**Data Protection Issue**	**Statutory Provisions**	**Retention Period**	**Action at End of Administrative Life of Record**
4.12	Accessibility strategy	Yes	Special Educational Needs and Disability Act 2001 Section 14	Closure + 12 years	Secure disposal unless legal action is pending
4.13	Parental permission slips for school trips, where there has been no major incident	Yes		Conclusion of the trip	Secure disposal unless legal action is pending
4.14	Parental permission slips for school trips, where there has been a major incident	Yes	Limitation Act 1980	Date of birth of pupil involved in the incident + 25 years	Secure disposal. Permission slips for all pupils on trip need to be retained for

					period to show that the rules had been followed for all pupils.
4.15	Walking bus registers	Yes		Date of register + 3 years	This takes into account that if an incident requiring an accident report, the register will be submitted with the accident report and kept for the retention time for accident reporting. Secure disposal

5) Curriculum

	Basic File Description	Data Protection Issue	Statutory Provisions	Retention Period	Action at End of Administrative Life of Record
5.1	School development plan	No		Current year + 6 years	Secure disposal
5.2	Schemes of work	No	The Education (School Records) Regulations 1989. Regulation 3 of the Education (Pupil Information) (England) Regulations 2005.	Current year + 1 year	It may be appropriate to review these records at end of each year and allocate a new retention period. Secure disposal.
5.3	Timetable	No		Current year + 1 year	It may be appropriate to review these records at end of each year and allocate a new retention period. Secure disposal.
5.5	Planning books	Yes/No		Current year + 1 year	It may be appropriate to review these records at end of each year and allocate a new retention period. Secure disposal.
5.6	Mark books	Yes/No		Current year + 1 year	It may be appropriate to review these records at end of each year and allocate a new retention period. Secure disposal.
5.7	Record of homework set	No		Current year + 1 year	It may be appropriate to review these records at end of each year and allocate a new retention period. Secure disposal.
5.8	Pupils' work	Yes		Current year + 1 year	It may be appropriate to review these records at end of each year and allocate a new retention period. Secure disposal.
5.9	Examination results	Yes		Current year + 6 years	Secure disposal

5.10	SATs records, examination papers and results	Yes		Current year + 6 years	Secure disposal
5.11	Value added and contextual data	Yes		Current year + 6 years	Secure disposal

6) Personnel Records held in Schools

	Basic File Description	Data Protection Issue	Statutory Provisions	Retention Period	Action at End of Administrative Life of Record
6.1	Staff personnel files	Yes		Termination + 6 years	Secure disposal
6.2	Interview notes and recruitment records	Yes		Date of interview notes + 6 months if unsuccessful. If successful place in personnel file.	Secure disposal
6.3	Pre-employment vetting information (including DBS checks)	Yes	DBS guidelines	Date of check + 6 months DBS only - Destroy once decision made (retain outcome only)	Secure disposal
6.4	Disciplinary proceedings	Yes	Where the warning relates to child protection issues see 1.2	Disciplinary: Expiry of warning unless safeguarding-related	
6.4a	*Formal Verbal Warning*	Yes		Date of warning + 6 months	Secure disposal
6.4b	*Formal Written warning*	Yes		Date of warning + 6 months	Secure disposal
6.4c	*Final Written warning*	Yes		Date of warning + 12 months	Secure disposal
6.4d	*Final Dismissal*	Yes		Date of warning + 18 months	Secure disposal
6.4e	*Case not found*	Yes		If child protection see 1.2, otherwise destroy immediately	Secure disposal
6.6	Records relating to accident/injury at work	Yes		Pupil - DOB + 25 years Adult - Date + 7 years	In case of serious accidents a further retention period will need to be applied. Secure disposal
6.7	Annual appraisal and assessment records	Yes		Current year + 6 years	Secure disposal
6.8	Pay Slips	Yes		Last date of employment + 6 years	Secure disposal

6.9	Maternity pay records	Yes	Statutory Maternity Pay (General) Regulations 1986 (SI1986/1960), revised 1999 (SI 1999/567)	Current year + 3 years	Secure disposal

	Basic File Description	**Data Protection Issue**	**Statutory Provisions**	**Retention Period**	**Action at End of Administrative Life of Record**
6.10	Records held under Retirement Benefits Schemes (Information Powers) Regulations 1995	Yes		Current year + 6 years	Secure disposal
6.11	Proofs of identity collected as part of DBS check	Yes		Where possible these should be checked and a note/copy of what was checked placed on personnel file. If felt necessary to keep any documentation this should also be placed in personnel file.	Secure disposal of notes/copies and return of originals.

7) Health and Safety

	Basic File Description	Data Protection Issue	Statutory Provisions	Retention Period	Action at End of Administrative Life of Record
7.1	Accessibility plans	Yes	Disability Discrimination Act	Current year + 6 years	Secure disposal
7.2	Accident reporting		Social Security (Claims and Payments) Regulations 1979 Regulation 25. Social Security Administration Act 1992 Section 8. Limitation Act 1980	Current year + 3 years	Secure disposal
7.2a	Adults	Yes		Date of incident + 7 years	Secure disposal
7.2b	Children	Yes		Date of birth of child + 25 years	Secure disposal
7.3	COSHH	Yes		Current year + 10 years Where appropriate an additional retention period may be allocated.	Secure disposal
7.4	Incident reports	Yes		Current year + 20 years	Secure disposal
7.5	Policy statements	No		Date of expiry + 1 year	Secure disposal
7.6	Risk assessments	No		Current year + 3 years	Secure disposal
7.7	Process of monitoring areas where employees and persons are likely to have come in contact with asbestos	No		Last action + 40 years	Secure disposal
7.8	Process of monitoring areas where employees and persons are likely to have come in contact with radiation	No		Last action + 50 years	Secure disposal
7.9	Fire precautions log book	No		Current year + 6 years	Secure disposal

8) Administrative

	Basic File Description	Data Protection Issue	Statutory Provisions	Retention Period	Action at End of Administrative Life of Record
8.1	Employer's liability certificate	No		Closure of school + 40 years	Secure disposal
8.2	Inventories of equipment and furniture	No		Current year + 6 years	Secure disposal
8.3	General file series	No		Current year + 5 years	Review to see if further retention period required. Secure disposal
8.4	School brochure or prospectus	No		Current year + 3 years	Disposal
8.5	Circulars (staff, parents, pupils)	Yes		Current year + 1 year	Review to see if further retention period required. Secure disposal
8.6	Newsletters, ephemera	No		Current year + 1 year	Review to see if further retention period required. Secure disposal
8.7	Visitors book	Yes		Current year + 2 year	Review to see if further retention period required. Secure disposal
8.8	PTA/Old Pupils Associations	Yes		Current year + 6 years	Review to see if further retention period required. Secure disposal

9) Finance

	Basic File Description	Data Protection Issue	Statutory Provisions	Retention Period	Action at End of Administrative Life of Record
9.1	Annual accounts	No	Financial Regulations	Current year + 6 years	Secure disposal
9.2	Loans and grants	Yes	Financial Regulations	Date of last payment on loan + 12 years	Secure disposal
9.3	Contracts	Yes	Section 2 of the Limitation Act 1980.		
9.3a	*Under seal*	Yes		Contract completion date + 12 years	Secure disposal
9.3b	*Under signature*	Yes		Contract completion date + 6 years	Secure disposal
9.3c	*Monitoring records*	Yes		Current year + 2 years	Secure disposal
9.4	Copy orders	No		Current year + 2 years	Secure disposal
9.5	Budget reports, budget monitoring etc.	No		Current year + 3 years	Secure disposal
9.6	Invoice, receipts and other records covered by the Financial Regulations, including VAT	No	Financial Regulations Record keeping (VAT Notice 700/21).	Current year + 6 years	Secure disposal
9.7	Annual budget and background papers	No		Current year + 6 years	Secure disposal
9.8	Order books and requisitions	No		Current year + 6 years	Secure disposal
9.9	Delivery documentation	No		Current year + 6 years	Secure disposal
9.10	Debtors' records	Yes	Limitations Act	Current year + 6 years	Secure disposal
9.11	School fund - Cheque books	Yes		Current year + 3 years	Secure disposal
9.12	School fund - Paying in books	Yes		Current year + 6 years	Secure disposal
9.13	School fund - Ledger	Yes		Current year + 6 years	Secure disposal
9.14	School fund - Invoices	Yes		Current year + 6 years	Secure disposal
9.15	School fund - Receipts	Yes		Current year + 6 years	Secure disposal
9.16	School fund - Bank statements	Yes		Current year + 6 years	Secure disposal
9.17	Student grant applications	Yes		Current year + 3 years	Secure disposal
9.18	Petty cash books	Yes		Current year + 6 years	Secure disposal

10) Property

	Basic File Description	Data Protection Issue	Statutory Provisions	Retention Period	Action at End of Administrative Life of Record
10.1	Title deeds	No		Permanent	These should follow the property
10.2	Plans	No		Permanent	Retain in school whilst operational. Can then be archived/stored elsewhere.
10.3	Maintenance and contractors	Yes	Financial Regulations	Current year + 6 years	Secure disposal
10.4	Leases	No		Expiry of lease + 6 years	Secure disposal
10.5	Lettings	No		Current year + 3 years	Secure disposal
10.6	Burglary, theft and vandalism report forms	Yes		Current year + 6 years	Secure disposal
10.7	Maintenance log books	No		Last entry + 10 years	Secure disposal
10.8	Contractors' reports	Yes		Current year + 6 years	Secure disposal

11) Department for Education

	Basic File Description	Data Protection Issue	Statutory Provisions	Retention Period	Action at End of Administrative Life of Record
11.1	HMI reports	Yes		These do not need to be kept any longer	Secure disposal
11.2	OFSTED, ISI reports and papers	No		Replace former report with new inspection report	Review to see if further retention period required. Secure disposal
11.3	Circulars from Department of Education	No		Whilst required operationally	Review to see if further retention period required. Disposal

12) Outside Agencies (related to Learning Support Department)

	Basic File Description	Data Protection Issue	Statutory Provisions	Retention Period	Action at End of Administrative Life of Record
12.1	Reports for outside agencies - where the report has been included on the case file created by the outside agency	Yes		Whilst the child is attending the school	Secure disposal

Secure Disposal Notes

- Paper records: shredded or incinerated.
- Electronic records: permanently deleted, including from cloud systems and backups, with confirmation logs where possible.
- Third-party providers: must provide deletion certificates or written confirmation of secure disposal.

Appendix 3:

Data Protection Impact Assessment

As part of our commitment to safeguarding pupils' personal information, the school carries out **Data Protection Impact Assessments (DPIAs)** before introducing any new system, technology, or activity that involves the use of personal data. A DPIA is a risk assessment that helps the school identify how personal information may be collected, stored, and shared, and ensures that appropriate measures are in place to protect it. This process allows the school to balance the benefits of new technologies with the responsibility to keep pupils, parents, and staff safe, in line with UK GDPR and data protection law.

Dolphin School Trust

Date: _____

Completed by: _____

1. Project Summary	*What is being introduced/changed? Why?*			
2. Data Involved	**Data subjects:**	*(e.g., pupils, parents, staff)*	**Data items:**	*(e.g., names, photos, contact details*
3. Purpose and Legal Basis	**Purpose:**	*Why is the data being processed?*		

	Lawful basis:	*(Public task / Consent / Contract / Legal obligation / Legitimate interests)*		
	Special category data?	*(Yes/No – if yes, state condition under Article 9 UK GDPR)*		
4. Risks & Mitigation	**Risk**	**Likelihood**	**Impact**	**Control in Place**
	Example: Photo shared without consent	*Low*	*Medium*	*Clear consent process, staff reminders*
5. Decision	Approved / Approved with conditions / Not approved			
Signed: _____ (Headteacher / DPO) **Date:** _____				