



## Batford Day Care

### BATFORD DAY CARE LIMITED DATA PROTECTION POLICY

|                                    |                     |
|------------------------------------|---------------------|
| <b>Version</b>                     | 2.0                 |
| <b>Based on Statutory Guidance</b> | Schools DPO Service |
| <b>Review body:</b>                | Day Care Manager    |
| <b>Date issued:</b>                | December 2024       |
| <b>Review frequency:</b>           | Two years           |
| <b>Target audience:</b>            | All stakeholders    |

| <b>Version</b> | <b>Date</b>   | <b>Notes</b> |
|----------------|---------------|--------------|
| V2.0           | December 2024 | New Format   |
|                |               |              |
|                |               |              |

Batford Day Care is committed to:

- Safeguarding and promoting the welfare of children and young people and expects all staff and volunteers to share this commitment.
- Eliminating discrimination, advancing equality of opportunity and fostering good relations between different groups. These factors were considered in the formation and review of this policy and will be adhered to in its implementation and application across the whole Batford Day Care community.
- Promoting the fundamental British values of democracy, the rule of law, individual liberty and mutual respect and tolerance of those with different faiths and beliefs: any day care member or visitor expressing opinions contrary to fundamental British Values, including 'extremist' views, will be actively challenged.

**BUILDING STRONG FOUNDATIONS FOR OUR CHILDREN**

Batford Day Care, Holcroft Road, Harpenden AL5 5BQ

## Contents

|   |           |
|---|-----------|
| <b>1. Aims.....</b>   | <b>3</b>  |
| <b>2. Legislation and guidance .....</b>                                | <b>3</b>  |
| <b>3. Definitions .....</b>   | <b>3</b>  |
| <b>4. The Data Controller .....</b>                                     | <b>4</b>  |
| <b>5. Roles and Responsibilities .....</b>                              | <b>4</b>  |
| 5.1 Day Care Management Team .....                                      | 4         |
| 5.2 Data Protection Officer .....                                       | 4         |
| 5.3 Day Care Manager .....  | 4         |
| 5.4 All staff .....   | 4         |
| <b>6. Data protection principles .....</b>                              | <b>4</b>  |
| <b>7. Collecting personal data .....</b>                                | <b>5</b>  |
| 7.1 Lawfulness, fairness and transparency.....                          | 5         |
| 7.2 Limitation, minimisation and accuracy.....                          | 6         |
| <b>8. Sharing personal data.....</b>                                    | <b>6</b>  |
| <b>9. Subject access requests and other rights of individuals .....</b> | <b>6</b>  |
| 9.1 Subject access requests .....                                       | 6         |
| 9.2 Children and subject access requests.....                           | 7         |
| 9.3 Responding to subject access requests .....                         | 7         |
| 9.4 Other data protection rights of the individual .....                | 8         |
| <b>10. CCTV .....</b>   | <b>8</b>  |
| <b>11. Photographs and videos .....</b>                                 | <b>8</b>  |
| <b>12. Data protection by design and default .....</b>                  | <b>9</b>  |
| <b>13. Data security and storage of records.....</b>                    | <b>9</b>  |
| <b>14. Disposal of records .....</b>                                    | <b>10</b> |
| <b>15. Personal data breaches .....</b>                                 | <b>10</b> |
| <b>16. Training.....</b>  | <b>10</b> |
| <b>17. Monitoring arrangements.....</b>                                 | <b>10</b> |
| <b>Appendix 1: Personal data breach procedure .....</b>                 | <b>11</b> |
| <b>Appendix 2: Data retention schedule.....</b>                         | <b>13</b> |

## 1. Aims

Batford Day Care aims to ensure that all personal data collected about staff, children, parents, directors, visitors and other individuals is collected, stored and processed in accordance with the [General Data Protection Regulation \(EU\) 2016/679 \(GDPR\)](#) and the [Data Protection Act 2018 \(DPA 2018\)](#).

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 GDPR and the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the [GDPR](#).

It also reflects the ICO's [code of practice](#) for the use of surveillance cameras and personal information.

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

| Term                                | Definition   |
|-------------------------------------|--|
| Personal data                       | Any information relating to an identified, or identifiable, living individual.<br>This may include the individual's: <ul style="list-style-type: none"><li>• Name (including initials)</li><li>• Identification number</li><li>• Location data</li><li>• Online identifier, such as a username</li></ul> 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: <ul style="list-style-type: none"><li>• Racial or ethnic origin</li><li>• Political opinions</li><li>• Religious or philosophical beliefs</li><li>• Trade union membership</li><li>• Genetics</li><li>• Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes</li><li>• Health – physical or mental</li><li>• Sex life or sexual orientation</li></ul> |
| Processing                          | Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying.<br>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

Batford Day Care processes personal data relating to parents, children, staff, directors, visitors and others, and therefore is a data controller.

Batford Day Care is registered with the ICO.

## 5. Roles and Responsibilities

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

### 5.1 Day Care Management Team

Batford Day Care's Management Team has overall responsibility for ensuring that Batford Day Care complies with all relevant data protection obligations.

### 5.2 Data Protection Officer

The Data Protection Officer (DPO) (Zoe Price) is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable.

The DPO is also the first point of contact for individuals whose data the day care processes, and for the ICO.

This post is held by the Day Care Business Manager. The DPO can be contacted at:

zoe.price@batfordnursery.herts.sch.uk

### 5.3 Day Care Manager

The Day Care Manager acts as the representative of the data controller on a day-to-day basis.

### 5.4 All staff

Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Informing the day care of any changes to their personal data, such as a change of address
- Contacting the DPO in the following circumstances:
  - With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
  - If they have any concerns that this policy is not being followed
  - If they are unsure whether 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 Batford Day Care 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 Batford Day Care 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:

- The data needs to be processed so that the Batford Day Care can **fulfil a contract** with the individual, or the individual has asked Batford Day Care to take specific steps before entering into a contract
- The data needs to be processed so that the Batford Day Care can **comply with a legal obligation**
- The data needs to be processed to ensure the **vital interests** of the individual or another person, *i.e.* to protect someone's life
- The data needs to be processed so that the day care as a public authority, can **perform a task in the public interest or exercise its official authority**
- The data needs to be processed for the **legitimate interests** of Batford Day Care (where the processing is not for any tasks Batford Day Care performs as a public authority) or a third party, provided the individual's rights and freedoms are not overridden
- The individual (or their parent/carer 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 under data protection law:

- The individual (or their parent/carer in the case of a child) has given **explicit consent**
- The data needs to be processed to perform or exercise obligations or rights in relation to **employment, social security or social protection law**
- The data needs to be processed to ensure the **vital interests** of the individual or another person, where the individual is physically or legally incapable of giving consent
- The data has already been made **manifestly public** by the individual
- The data needs to be processed for the establishment, exercise or defence of **legal claims**
- The data needs to be processed for reasons of **substantial public interest** as defined in legislation
- The data needs to be processed for **health or social care purposes**, and the processing is done by, or under the direction of, a health or social work professional or by any other person obliged to confidentiality under law
- The data needs to be processed for **public health reasons**, and the processing is done by, or under the direction of, a health professional or by any other person obliged to confidentiality under law
- The data needs to be processed for **archiving purposes**, scientific or historical research purposes, or statistical purposes, and the processing is in the public interest

For criminal offence data, we will meet both a lawful basis and a condition set out under data protection law. Conditions include:

- The individual (or their parent/carer in the case of a child) has given **consent**
- The data needs to be processed to ensure the **vital interests** of the individual or another person, where the individual is physically or legally incapable of giving consent
- The data has already been made **manifestly public** by the individual

- The data needs to be processed for or in connection with legal proceedings, to obtain legal advice, or for the establishment, exercise or defence of **legal rights**
- The data needs to be processed for reasons of **substantial public interest** as defined in legislation

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

We will always consider the fairness of our data processing. We will ensure we do not handle personal data in ways that individuals would not reasonably expect or use personal data in ways which have unjustified adverse effects on them.

## **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.

We will keep data accurate and, where necessary, up to date. Inaccurate data will be rectified or erased when appropriate.

In addition, 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 Batford Day Care's record retention schedule.

## **8. Sharing personal data**

We will not normally share personal data with anyone else without consent, but there are certain circumstances where we may be required to do so. These include, but are not limited to, situations where:

- There is an issue with a child 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 children – 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 contract with the supplier or contractor 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

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

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

Where we transfer personal data internationally, 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 Batford Day Care 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 is not possible, the criteria used to determine this period
- Where relevant, the existence of the right to request rectification, erasure or restriction, or to object to such processing
- The right to lodge a complaint with the ICO or another supervisory authority
- 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
- The safeguards provided if the data is being transferred internationally

Subject access requests can be submitted in any form, but we may be able to respond to requests more quickly if they are made in writing and include:

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

If staff receive a subject access request in any form, they must immediately forward it to the DPO.

## **9.2 Children and subject access requests**

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

Children 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, given the age range of children at Batford Day Care, subject access requests from parents or carers of pupils will be granted without the express permission of the child.

## **9.3 Responding to subject access requests**

When responding to requests, we:

- May ask the individual to provide two forms of identification
- May contact the individual via phone to confirm the request was made
- Will respond without delay and within one month of receipt of the request (or receipt of the additional information needed to confirm identity, where relevant)
- Will provide the information free of charge
- May tell the individual we will comply within three months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within one month, and explain why the extension is necessary

We may not disclose information for a variety of reasons, such as if it:

- Might cause serious harm to the physical or mental health of the child or another individual
- Would reveal that the child is being or has been abused, or is at risk of abuse, where the disclosure of that information would not be in the child's best interests

- Would include another person's personal data that we cannot reasonably anonymise, and we do not have the other person's consent and it would be unreasonable to proceed without it
- Is part of certain sensitive documents, such as those related to crime, immigration, legal proceedings or legal professional privilege, management forecasts, negotiations, confidential references, or exam scripts

If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee to cover administrative costs. We will take into account whether the request is repetitive in nature when making this decision.

When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO or they can seek to enforce their subject access right through the courts.

#### **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 (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Object to processing which has been justified on the basis of public interest, official authority or legitimate interests
- Challenge decisions based solely on automated decision making or profiling (*i.e.* making decisions or evaluating certain things about an individual based on their personal data with no human involvement)
- Be notified of a data breach (in certain circumstances)
- Make a complaint to the ICO
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)

Individuals should submit any request to exercise these rights to the DPO. If staff receive such a request, they must immediately forward it to the DPO.

## **10. CCTV**

We use CCTV in various locations around the nursery school and day care site to ensure it remains safe. We will adhere to the ICO's [code of practice](#) for the use of CCTV.

We do not need to ask individuals' permission to use CCTV, but we make it clear where individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use.

Any enquiries about the CCTV system should be directed to the DPO.

## **11. Photographs and videos**

As part of Batford Day Care activities, we may take photographs and record images of individuals within our day care.

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 child.

Any photographs and videos taken by parents/carers at Batford Day Care events for their own personal use are not covered by data protection legislation. However, we will ask that photos or videos with other children

are not shared publicly on social media for safeguarding reasons, unless all the relevant parents/carers have agreed to this.

Where Batford Day Care takes photographs and videos, uses may include:

- Within Batford Day Care on notice boards and in brochures, newsletters, etc.
- Outside of Batford Day Care by external agencies such as the external photographer, newspapers, campaigns
- Online on our website or social media pages

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

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

## **12. Data protection by design and default**

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

- Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge
- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law (*see Section 6*)
- Completing data protection impact assessments where Batford Day Care'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
- Appropriate safeguards being put in place if we transfer any personal data outside of the European Economic Area (EEA), where different data protection laws will apply
- Maintaining records of our processing activities, including:
  - For the benefit of data subjects, making available the name and contact details of Batford Day Care 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, type of data subject, how and why we are using the data, any third-party recipients, any transfers outside of the EEA and the safeguards for those, retention periods and how we are keeping the data secure

## **13. 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 desks, on staffroom tables, or left anywhere else where there is general access
- Passwords that are complex; containing letters and numbers are used to access Batford Day Care computers, laptops and other electronic devices. Staff are reminded that they should not reuse passwords from other sites
- Encryption software is used to protect portable devices and removable media, such as laptops and USB devices
- As a rule, staff and directors should not store work related information on personal devices and should save documents only to the server. Where staff or directors store work related information on their personal devices, they are expected to follow the same security procedures as for Batford Day Care owned equipment (see our online safety policy and acceptable use agreements)
- 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*)

## **14. 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 Batford Day Care's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

## **15. Personal data breaches**

Batford Day Care 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 after becoming aware of it. Such breaches may include, but are not limited to:

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

## **16. Training**

All staff 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 Batford Day Care's processes make it necessary.

## **17. Monitoring arrangements**

The DPO is responsible for monitoring and reviewing this policy. This policy will be reviewed every two years and shared with Batford Day Care staff.

## Appendix 1: Personal data breach procedure

This procedure is based on [guidance on personal data breaches](#) produced by the ICO.

- On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the DPO
- The DPO will investigate the report and determine whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidentally or unlawfully:
  - Lost
  - Stolen
  - Destroyed
  - Altered
  - Disclosed or made available where it should not have been
  - Made available to unauthorised people
- The DPO will alert the Day Care Manager and the board of directors
- The DPO will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary (actions relevant to specific data types are set out at the end of this procedure)
- The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen
- The DPO will work out whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the DPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:
  - Loss of control over their data
  - Discrimination
  - Identify theft or fraud
  - Financial loss
  - Unauthorised reversal of pseudonymization (for example, key-coding)
  - Damage to reputation
  - Loss of confidentiality
  - Any other significant economic or social disadvantage to the individual(s) concerned

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

- The DPO will document the decision (either way), in case it is challenged at a later date by the ICO, or an individual affected by the breach. Documented decisions are stored.
- Where the ICO must be notified, the DPO will do this via the ['report a breach' page](#) of the ICO website, or through their breach report line (0303 123 1113), within 72 hours. As required, the DPO will set out:
  - A description of the nature of the personal data breach including, where possible:
  - The categories and approximate number of individuals concerned
  - The categories and approximate number of personal data records concerned
  - The name and contact details of the DPO
  - A description of the likely consequences of the personal data breach
  - A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned

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

- The DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPO will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:
  - A description, in clear and plain language, of the nature of the personal data breach
  - The name and contact details of the DPO
  - A description of the likely consequences of the personal data breach
  - A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned

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

- The DPO will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies
- The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:
  - Facts relating to the breach
  - Effects
  - Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)

Records of all breaches will be stored.

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

### **Actions to minimise the impact of data breaches**

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

- If special category data is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error
- Members of staff who receive personal data sent in error must alert the sender and the DPO as soon as they become aware of the error
- If the sender is unavailable or cannot recall the email for any reason, the DPO will ask the ICT department to recall it
- In any cases where the recall is unsuccessful, the DPO will contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way
- The DPO will ensure we receive a written response from all the individuals who received the data, confirming that they have complied with this request
- The DPO will carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted

## Appendix 2: Data retention schedule

| Management Data   |   |   |   |                         |
|---|---|---|---|-------------------------|
| Record  | File Action                                 | Minimum Retention Period  | Statutory Provision                       | Action After Retention  |
| Board of Directors – general correspondence   | Close at end of current financial year      | Current year + 3 years  |   | Destroy                 |
| Board of Directors Meetings Minutes (master)  | Close at end of current financial year      | 10 years from the date of the meeting   |   | Destroy                 |
| Staff Meeting Minutes   | Close at end of current financial year      | Normal Review   |   | Determination on Review |
| Day Care Development Plan   | Retain whilst valid – close when superseded | Life of the plan + 3 years  |   | Destroy                 |
| Policy Statements (Data Protection, Internet, Health & Safety, Child Protection, Equality etc.) | Retain whilst valid – close when superseded | Review regularly & retain latest version<br>Older versions: date of expiry + 1 year |   | Destroy                 |
| Visitors Book   | Close at end of current school year (BNS)   | End of current year + 1 years   |   | Destroy                 |
| Comments/Complaints   | Close at end of current financial year      | Date of resolution of complaint + 6 years   |   | Archive                 |
| Emergency Planning/Business Continuity Plan   | Retain whilst valid – close when superseded | Until superseded  |   | Destroy                 |
| CCTV  | Overwritten automatically (BNS)             | 30 days   | Surveillance Camera Code of Practice 2021 | Delete                  |

| Child data  |  |   |   |                        |
|---|--|---|---|------------------------|
| Record  | File Action  | Minimum Retention Period  | Statutory Provision   | Action After Retention |
| Child file and records that contribute to the child record  | Close when child leaves setting and either archived or sent to child's onwards destination | Primary - Retain whilst the child remains at the primary school<br>Secondary - Date of birth of the pupil + 25 years  | The Education (Pupil Information) (England) Regulations<br>2005 SI 2005 No. 1437 As amended by SI 2018 No 688<br>Limitation Act 1980 (Section 2)  |                        |
| Child Attendance Registers  | Retain in secure, confidential storage   | Date of birth of the pupil + 25 years   | School attendance: Departmental advice for maintained schools, Academies, independent schools and local authorities 2014  | Destroy                |
| Special Education Needs files, reviews and Education, Health and Care Plan, including advice and information provided to parents regarding educational needs and accessibility strategy | Retain in secure, confidential storage   | Date of birth of the child + 31 years [Education, Health and Care Plan is valid until the individual reaches the age of 25 years<br>– the retention period adds an additional 6 years from the end of the plan in line with the Limitation Act] | Children and Family's Act 2014;<br>Special Educational Needs and Disability Act 2001 Section 14   | Destroy                |
| Child Protection  | Retain in secure, confidential storage   | Until child is 25 years old   | "Keeping children safe in education Statutory guidance for schools and colleges";<br>"Working together to safeguard children. A guide to inter-agency working to safeguard and promote the welfare of children" | Destroy                |
| Disciplinary Action (Suspension/Expulsion)/Offences – bullying  | Close when child leaves setting  | Lifetime of child file  |   | Destroy                |
| Medical Records – records of pupils with medical conditions and details for the administration of drugs when necessary.   | Close when child leaves setting  | Until child is 22 years old or in the case of a Special Needs child, until 25 years old   |   | Destroy                |

| Personnel data  |   |   |   |                              |
|---|---|---|---|------------------------------|
| Record  | File Action                               | Minimum Retention Period  | Statutory Provision   | Action After Retention       |
| Staff Personnel Records (including recruitment, interview notes, appointment details, training, staff development etc.) | Close when member of staff leaves setting | During validity + 6 years after leaving employment  | Limitation Act 1980 (Section 2)   | Destroy                      |
| Staff Salary Records  | Close at end of current financial year    | Last Day of Employment + 85 Years   |   | Archive for Pension purposes |
| Staff Sickness Records (copies of Medical Certs)  | Close at end of current financial year    | Current academic year + 6 years   |   | Destroy                      |
| Agency Staff Records  | Close at end of current financial year    | Current financial year + 6 years  |   | Destroy                      |
| Student Records (e.g. nursery assistant students & pupils from schools on work experience)                              | Close at end of current financial year    | Current financial year + 6 years  |   | Destroy                      |
| Procedures for Induction of Staff   |   | Until superseded  |   | Destroy                      |
| Staff Performance Review  | Close at end of review period covered     | During validity   |   | Destroy                      |
| Records relating to any allegation of a child protection nature against a member of staff                               |   | Until the person's normal retirement age or 10 years from the date of the allegation (whichever is the longer) then REVIEW. | Keeping children safe in education Statutory guidance for schools and colleges; Working together to safeguard children. A guide to inter-agency working to safe-guard and promote the welfare of children |                              |

| Finance data  |  |   |                     |  |
|---|--|---|---------------------|--|
| Record  | File Action                            | Minimum Retention Period                  | Statutory Provision | Action After Retention                       |
| Annual Budget   | Close at end of current financial year | Current financial year + 6 years          |                     | Destroy                                      |
| Budget Monitoring   | Close at end of current financial year | Current financial year + 3 years          |                     | Destroy                                      |
| Annual Accounts   | Close at end of current financial year | Current financial year + 6 years          |                     | Archive                                      |
| Order Books, Invoices, Bank Records, Cash Books, Till Rolls, Lodgement books etc. | Close at end of current financial year | Current financial year + 6 years          |                     | Destroy                                      |
| Postage Book  | Close at end of current financial year | Current financial year + 6 years          |                     | Destroy                                      |
| Purchasing – Tender Information & Prices  |  | Until superseded                          |                     | Destroy contract schedules when they expire. |
| Audit Reports   | Close at end of current financial year | Current financial year + 6 years          |                     | Destroy                                      |
| All records relating to the management of contracts under signature               |  | Last payment on the contract<br>+ 6 years | Limitation Act 1980 | Destroy contract when they expire.           |

| Health and Safety                                   |                                |  |   |                                   |
|---|--------------------------------|--|---|-----------------------------------|
| Record  | File Action                    | Minimum Retention Period   |   | Action After Retention            |
| Accident / Incident Book                            | Close after last entry in book | Date of closure + 12 years   | Social Security (Claims and Payments) Regulations 1979 Regulation 25.   | Destroy                           |
| Legal /Accident/Incident Forms                      |                                | Until child is at least 22 years old or in the case of an adult 4 years from the date of the accident  | Social Security Administration Act 1992 Section 8.<br>Limitation Act 1980<br>Social Security (Claims and Payments) Regulations 1979.<br>SI 1979 No 628 Social Security (Claims and Payments) Regulations<br>SI 1987 No 1968 Revokes all but Part 1 of SI 1979 No 628<br>Social Security Administration Act 1992 Section 8.<br>Social Security (Claims and Payments) Amendment (No 30 Regulations 1993<br>SI 1993 No 2113 Allows the information to be kept electronically | Destroy                           |
| Risk Assessments – work experience locations/pupils |                                | Life of risk assessment + 3 years provided that a copy of the risk assessment is stored with the accident report if an incident has occurred |   | Destroy                           |
| H & S Reports                                       |                                | Current Year + 20 years  |   | Destroy                           |
| Fire Procedure                                      |                                | Until superseded   |   | Retain copies of earlier versions |
| Security System File                                |                                | For the life of the system   |   | Destroy                           |
| H&S Policy Statement                                |                                | Date of expiry + 1 Year  |   | Destroy                           |