# Data Protection Policy 2023-24

## Contents

## 1. Aims

Northleigh House School aims to ensure that all personal data collected about staff, pupils, parents, trustees, visitors, and other individuals is collected, stored and processed in accordance with the General Data Protection Regulation (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 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.

It 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, individual.<br>This may include the individual's:<br>• Name (including initials)<br>• Identification number<br>• Location data<br>• Online identifier, such as a username<br>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:<br>• Racial or ethnic origin<br>• Political opinions<br>• Religious or philosophical beliefs<br>• Trade union membership<br>• Genetics<br>• Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes<br>• Health – physical or mental<br>• 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.<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

Northleigh House School processes personal date relating to parents, students, staff, volunteers, visitors, and others, and therefore is a data controller. Northleigh's House 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 Northleigh House School, and to external organisations, volunteers and other individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action.

### 5.1 Board of Trustees

The Board of Trustees has overall responsibility for ensuring that Northleigh House School complies with all relevant data protection obligations.

### 5.2 Data Protection Advice and Guidance

The Compliance Officer is responsible for providing advice and guidance to Northleigh House School to assist the school to implement this policy, monitor compliance with data protection law, and develop related policies and guidelines where applicable. The Compliance Officer along with a member of the senior management team will carry out an annual audit of Northleigh House School's data processing activities and report to the Board of Trustees their advice and recommendations on school data protection issues. The Compliance Officer is also the first point of contact for individuals whose data the school processes, and for the ICO.

### 5.3 School Director

The School Director acts as the representative of the data controller on a day-to-day basis.

### 5.4 Data Protection Lead

Northleigh House School has nominated the following individual as designated person to be contacted internally in relation to all matters relating to data protection issues, and to make referrals, where necessary. To: Viv Morgan on viv@northleigh.co.uk should they be unavailable then issues should be referred to a member of the senior management team.

### 5.5 All Staff

All members of 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 School Director/Data Protection Lead 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 UK.
    - 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. Northleigh House School has adopted the principles to underpin its Data Protection Policy: The principles require that all personal data shall be:
(1) processed lawfully, fairly and in a transparent manner ('lawfulness, fairness and transparency').
(2) used for specified, explicit and legitimate purposes ('purpose limitation').
(3) used in a way that is adequate, relevant, and limited to what is necessary ('data minimisation').
(4) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, are erased or rectified without delay ('accuracy').
(5) kept no longer than is necessary ('storage limitation').
(6) processed in a manner that ensures it is safe and secure, ensuring that measures against unauthorised or unlawful processing and against accidental loss, destruction or damage are in place ('integrity and confidentiality').
This policy sets out how the school aims to comply with these principles.

## 7. Collecting Personal Data

### 7.1 Lawfulness, Fairness and Transparency

Northleigh House School shall only process personal data where it has one of 5 'lawful bases' (legal reasons) available to the school 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 a contract.
- The data needs to be processed so that the school can **comply with a legal obligation.**
- The data needs to be processed to ensure the **vital interests** of the individual e.g., to protect someone's life.
- The data needs to be processed so that the school, as a public authority, can perform a task **in the public interest,** and carry out its official functions.
- The individual (or their parent/carer when appropriate in the case of a pupil) has freely given clear **consent**.

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

### 7.2 Limitation, Minimisation and Accuracy

We will only collect personal data for specified explicit and legitimate reasons. We will explain these reasons to the individuals when we first collect their data. If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so and seek consent where necessary.

Staff must only process personal data where it is necessary to do their jobs.

When staff no longer need the personal data they hold, they must ensure it is deleted or anonymised.

## 8. Sharing Personal Data

We will not normally share personal data with anyone else, except, as set out in the School's Privacy Notice. GDPR and the DPA 2018 also allow information to be shared 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 that affects any of our pupils or staff. Where we transfer personal data to a country or territory outside the UK, we will do so in accordance with 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 may be submitted in writing and can be sent either to the School Director, Chair of Trustees, Compliance Officer, Data Protection Lead, to a member of staff or a Trustee.

To enable the request to be accurately responded to, the applicant should be encouraged to make the request in writing and to set out:

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

The Compliance Officer will send the subject access request to the Data Protection Lead. If staff receive a subject access request, they must immediately forward it to the Data Protection Lead, who will ensure that the School Director/Chair of Trustees is informed. Information to be released will be collated by the school and then sent to the School Director/Data Protection Lead for checking and sending out to the applicant.

**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 person should have parental responsibility for the child, and the child must either be unable to understand their rights and the implications of a subject access request or have given their consent.

Children aged 13 and above are generally regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, subject access requests from those with parental responsibility for pupils at our school aged 13 and above may not be granted without the express permission of the pupil.

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, subject access requests from those with parental responsibility for pupils at our school will in general be granted without requiring the express permission of the pupil. These are not fixed rules 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 ask the individual to provide 2 forms of identification.
- May contact the individual via phone to confirm the request was made.
- Will respond without delay and within 1 month of receipt of the request.
- Will provide the information free of charge.
- May tell the individual we will comply within 3 months of receipt of the request, where a request is complex or numerous, or where it is impractical to comply within a month due to school closure. We will inform the individual of this within 1 month and explain why the extension is necessary.

We will not disclose information if it:

- Might cause serious harm to the physical or mental health of the pupil or another individual.

- Would reveal that the child is at risk of abuse, where the disclosure of that information would not be in the child's best interests.
- Is contained in adoption or parental order records.
- Is given to a court in proceedings concerning the child.

If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee which considers 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. If the school refuses 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, where processing is based on the consent of the pupil or parent.
- 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 based on 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 School Director. If staff receive such a request, they must immediately forward it to the Data Protection Lead who will send it to the School Director for information purposes.

## 10. CCTV

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

## 11. Photographs and Videos

As part of our school activities, Northleigh House School may take photographs and record images of individuals within the school. The school will obtain written consent from

parents/carers, or pupils aged 18 and over, for photographs and videos to be taken of pupils for communication, marketing, and promotional materials.

Where Northleigh House School needs parental consent, it shall clearly explain how the photograph and/or video will be used to both the parent/carer and pupil.
Where the School doesn't need parental consent, it shall clearly explain to the pupil how the photograph and/or video will be used.

Uses may include:

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

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

## 12. Data Protection by Design and Default

Northleigh House School shall put measures in place to show that it has integrated data protection into all its data processing activities, including:

- Appointing a suitably qualified person 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.
- Integrating data protection into internal documents including this policy, any related policies and privacy notices.
- 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.
- Maintaining records of our processing activities, including:
    - For the benefit of data subjects, making available the name and contact details of our school and Data Protection Lead 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.

## 13. Data Security and Storage of Records

Northleigh House School 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 (See **Appendix 2**).
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
- Staff must ensure passwords are difficult to guess by incorporating numbers, mixed case and special characters.
- Encryption software is used to protect all portable devices and removable media on which personal information is stored, such as laptops and USB devices
- Staff, pupils, or trustees who store personal information on their personal devices are expected to follow the same security procedures as for school-owned equipment
- 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.
For example, Northleigh House School will incinerate paper-based records, and overwrite or delete electronic files.

## 15. Personal Data Breaches

Northleigh House School shall take all reasonable steps 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, Northleigh House School shall report the data breach to the ICO within 72 hours. Such breaches in a school context may include, but are not limited to:

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

## 16. Training

All staff and trustees are provided with data protection training. Data protection will also form part of continuing professional development, where changes to legislation, guidance or the school's processes make it necessary.

## Review Date: September 2024

**Appendix 1**

## Personal Data Breach Procedures

If staff become aware that information has not been handled according to procedures and there is a data breach or potential security incident, they must report it in accordance with this procedure.

When appropriate, Northleigh House School will report the data breach to the ICO within 72 hours in accordance with the requirements of the GDPR legislation.

1. Data protection breaches occur where personal data is lost, damaged, destroyed, stolen, misused and/or accessed unlawfully.

2. Examples of how a breach may occur include:

    a. Theft of data or equipment on which data is stored.
    b. Loss of data or equipment on which data is stored.
    c. Inappropriate access controls allowing unauthorised use.
    d. Accidental Loss.
    e. Destruction of personal data.
    f. Damage to personal data.
    g. Equipment failure.
    h. Unlawful disclosure of personal data to a third party.
    i. Human error.
    j. Unforeseen circumstances such as fire or flood.
    k. Hacking attack; or
    l. 'Blagging' offences where information is obtained by deceiving the organisation which holds it.

3. If a member of staff of Northleigh House School, or a Trustee, discovers that data has been lost, or believes that there has been a breach of the data protection principles in the way that data is handled, you must immediately or no later than within 24 hours of first coming to notice, inform the School's Data Protection Lead.

4. Upon being notified, the School's Data Protection Lead will assess whether a breach of personal information has occurred, and the level of severity. If a breach has occurred but the risk of harm to any individual is low (for example, because no personal information has left the control of the school), then the School's Data Protection Lead will undertake an internal investigation to consider whether the Information Security Policy was followed, and whether any alterations need to be made to internal procedures as a result.

5. In all other cases, the incident must be notified to the Data Protection Lead immediately, who must follow the Information Commissioner's Office guidelines on notification and recording of the breach. The priority must then be to close or contain the breach to mitigate/minimise the risks to those individuals affected by it.

All Northleigh House School staff and Trustees are expected to work in partnership with the Data Protection Lead and the School Director in relation to the following matters:

**Notification of Breaches**
Any member of staff or Trustee who becomes aware of a personal information breach should provide full details to the Data Protection Lead for the School within 24 hours of being made aware of the breach.
The staff member made aware of the breach should complete a Personal Data Breach – Incident Form in detail and pass to the Data Protection Lead, who will advise of next steps and log on the Electronic Incident Log.

When completing the form details should be provided of the reporter's name, the date/time of the breach, the date/time of detecting the breach, and basic information about the type of breach and information about personal data concerned. Details of what has already been done to respond to the risks posed by the breach should also be included.

**Containment and Recovery**
The initial response is to investigate and contain the situation and a recovery plan including, damage limitation.

You may need input from specialists such as IT, HR and legal and in some cases contact with external third parties.

- Seek assistance in the containment exercise. This could be isolating or closing a compromised section of the network, recovery of released documents, finding a lost piece of equipment, or simply changing any related access codes
- Establish whether there is anything you can do to recover any losses and limit the damage the breach can cause.
- As well as the physical recovery of equipment, this could involve the use of backup records to restore lost or damaged data or ensuring that staff recognise when someone tries to use stolen data to access accounts.
- Consider whether any individual affected by the data breach should be notified.

**Assessing the Risks**
Levels of risk can be very different and vary on an individual breach of data security, depending on what is lost/damaged/stolen.

For example, if a case file is lost then risks are different depending on type of data and its sensitivity with potential adverse consequences for individuals. The Data Protection Lead should consider the following points:
- What type of data is involved?
- How sensitive is the data?
- If data has been lost or stolen, are there any protections in place such as encryption?
- What has happened to the data?
- If data has been stolen, could it be used for purposes which are harmful to the individuals to whom the data relate? If it has been damaged, this poses a different type and level of risk.
- Regardless of what has happened to the data, what could the data tell a third party about the individual? Sensitive data could mean very little to an opportunistic laptop thief while the loss of apparently trivial snippets of information could help a determined fraudster build up a detailed picture of other people
- How many individuals' personal data has been affected by the breach?
- Who are the individuals whose data has been breached?

- What harm can come to those individuals?
- Are there risks to physical safety or reputation, of financial loss or a combination of these and other aspects of their life?
- Are there wider consequences to consider such as a risk to life?
- Loss of public confidence in the school?

All staff and Trustees should establish whether there is anything they can do to recover any losses and limit the damage the breach can cause.

| Record Description | Data Protection Issues | Statutory Provisions | Retention information/period | Action at end of administrative life of the record (method of disposal) |
|---|---|---|---|---|
| **TRUSTEES** | | | | |
| Agendas for Trustees meetings | There may be data issues if the meeting is dealing with confidential issues relating to staff. | | One copy should be retained with the master set of minutes. All other copies can be disposed of. | SECURE DISPOSAL |
| Minutes of Trustee meetings<br><br>Principal Set (signed)<br><br>Inspection Copies | There may be data protection issues if the meeting is dealing with confidential issues relating to staff. | | PERMANENT<br><br>Date of meeting plus 3 years. | If the schools is unable to store these then they should be offered to the County Archives Service.<br><br>If these minutes contain any sensitive, personal information they must be shredded. |
| Reports presented to the Trustees | There may be data protection issues if the report deals with confidential issues relating to staff. | | Reports should be kept for a minimum of 6 years. However, if the minutes refer directly to individual reports then the reports should be kept permanently. | SECURE DISPOSAL or retained with the signed set of the minutes. |
| Trusts and Endowments managed by the Trustees | No | | PERMANENT | These should be retained in the school whilst the school is open and then |

| Record Description | Data Protection Issues | Statutory Provisions | Retention information/period | Action at end of administrative life of the record (method of disposal) |
|---|---|---|---|---|
| | | | | offered to County Archives Service when the school closes. |
| Action plans created and administered by the Trustees | No | | Life of the action plan plus 3 years. | SECURE DISPOSAL |
| Policy documents created and administered by the Trustees | No | | Life of the policy plus 3 years. | SECURE DISPOSAL |
| Records relating to complaints dealt with by the Trustees | Yes | | Life of the policy plus 3 years. | SECURE DISPOSAL |
| Annual Reports | No | The Charities Act 2011 Section 162<br>The Charities (Accounts and Reports) Regulations 2008 | Date of report plus 10 years. | SECURE DISPOSAL |
| Proposals concerning the change of status of the school | No | | Date proposal accepted or declined plus 3 years. | SECURE DISPOSAL |
| **SCHOOL DIRECTOR AND SENIOR MANAGEMENT TEAM** | | | | |
| Logbooks of activity in the school maintained by the School Director | There may be data protection issues if the logbook refers to individual pupils or members of staff (accident log). | | Date of last entry in the book and a minimum of 6 years then REVIEW. | SECURE DISPOSAL |

| Record Description | Data Protection Issues | Statutory Provisions | Retention information/period | Action at end of administrative life of the record (method of disposal) |
|---|---|---|---|---|
| Minutes of Senior Management Meetings and the meetings of other internal administrative bodies | There may be data protection issues if the minutes refers to individual pupils or members of staff. | | Date of the meeting and 3 years then REVIEW. | SECURE DISPOSAL |
| Reports created by the School Director or the Management Team | There may be data protection issues if the report refers to individual pupils or members of staff. | | Date of the report and a minimum of 3 years then REVIEW. | SECURE DISPOSAL |
| Records created by School Director, Heads of Department and other members of staff with administrative responsibilities | There may be data protection issues if the records refers to individual pupils or members of staff. | | Current academic year and 6 years then REVIEW. | SECURE DISPOSAL |
| Correspondence created by School Director, Heads of Department, and other members of staff with administrative responsibilities | There may be data protection issues if the correspondence refers to individual pupils or members of staff. | | Date of correspondence plus 3 years then REVIEW. | SECURE DISPOSAL |
| Provisional Development Plans | Yes | | Life of the plan plus 6 years. | SECURE DISPOSAL |
| School Development Plans | No | | Life of the plan plus 3 years. | SECURE DISPOSAL |
| **ADMISSIONS PROCESS** | | | | |
| Admissions Policy | No | | Life of policy plus 3 years then REVIEW. | SECURE DISPOSAL |
| Admissions – if the admission is successful | Yes | | This information should be added to the student file. Date of Birth of the student plus 25 years. | SECURE DISPOSAL |

| Record Description | Data Protection Issues | Statutory Provisions | Retention information/period | Action at end of administrative life of the record (method of disposal) |
|---|---|---|---|---|
| Admissions – if the admission is unsuccessful | Yes | | Resolution of case plus 3 months | SECURE DISPOSAL |
| Register of Admissions | Yes | | Every entry in the admission register must be preserved for a period of three years after the date on which the entry was made. | REVIEW<br>Schools may wish to consider keeping the admission register permanently as often school receive enquiries from past pupils to confirm the date, they attended the school. |
| Proof of address and Identification supplied by parents as part of the admissions process | Yes | | This information should be added to the student file. Date of Birth of the student plus 25 years. | SECURE DISPOSAL |
| Supplementary information form including additional information such as religion, medical conditions etc.<br>For successful admissions<br><br>For unsuccessful admissions | Yes | | <br>This information should be added to the student file. Date of Birth of the student plus 25 years.<br>3 months after unsuccessful admissions. | <br>SECURE DISPOSAL<br><br>SECURE DISPOSAL |

| Record Description | Data Protection Issues | Statutory Provisions | Retention information/period | Action at end of administrative life of the record (method of disposal) |
|---|---|---|---|---|
| **OPERATIONAL ADMINISTRATION** | | | | |
| General files | No | | Current year plus 5 years then REVIEW. | SECURE DISPOSAL |
| Records relating to the creation and publication of the school brochures or prospectus | No | | Current year plus 3 years. | STANDARD DISPOSAL |
| Records relating to the creation and distribution of circulars to staff, parents or students | No | | Current year plus 1 year. | STANDARD DISPOSAL |
| Newsletters and other items with a short operational use | No | | Current year plus 1 year. | STANDARD DISPOSAL |
| Visitors' Books and Signing in Sheets | Yes | | Current year plus 6 years then REVIEW. | SECURE DISPOSAL |
| Records relations to the creation and management of Parent Teacher Associations and/or Old Students Associations | No | | Current year plus 6 years then REVIEW. | SECURE DISPOSAL |
| **RECRUITMENT** | | | | |
| All records leading up to the appointment of a new School Director | Yes | | Date of appointment plus 6 years. | |

| Record Description | Data Protection Issues | Statutory Provisions | Retention information/period | Action at end of administrative life of the record (method of disposal) |
|---|---|---|---|---|
| All records leading up to the appointment of a new member of staff – unsuccessful candidates | Yes | | Date of appointment of successful candidate plus 6 months. | SECURE DISPOSAL |
| All records leading up to the appointment of a new member of staff – successful candidates | Yes | | All relevant information should be added to the Staff Personal File and all other information retained for 6 months. | SECURE DISPOSAL |
| Pre-employment vetting information – DBS Checks | No | DBS Update Service Employer Guide; Keeping Children Safe in Education | The school does not have to keep copies of DBS certificates, just certificate numbers once seen by a staff member. | |
| Proofs of identify collected as part of the process of checking "portable" enhanced DBS disclosure | Yes | | Where possible these documents should be added to the Staff Personal File. | |
| Pre-employment vetting information – Evidence proving right to work in the United Kingdom | Yes | An employer's guide to right to work checks – Home Office May 2015 | Where possible these documents should be added to the Staff Personal File. | |
| Staff/Trustee Personal File | Yes | Limitation Act 1980 Section 2 | Termination of Employment plus 6 years. | SECURE DISPOSAL |
| Volunteer File | Yes | | Current year plus 1 year. | SECURE DISPOSAL |
| Timesheets | Yes | | Current year plus 6 years. | SECURE DISPOSAL |

| Record Description | Data Protection Issues | Statutory Provisions | Retention information/period | Action at end of administrative life of the record (method of disposal) |
|---|---|---|---|---|
| Annual Appraisal Records | Yes | | Current year plus 5 years. | SECURE DISPOSAL |
| **MANAGEMENT OF DISCIPLINARY AND GRIEVOUS PROCESSES** | | | | |
| Allegation Of a child protection nature against a member of staff including where the allegation is unfounded | Yes | "Keeping children safe in education for schools and colleges"<br>"Working together to safeguard children. A guide to inter-agency working to safeguard and promote the welfare of children" | Until the person's normal retirement age or 10 years from the date of the allegation whichever is the longer then.<br>REVIEW – Note allegations that are found to be malicious should be removed from personnel files. If found, they are to be kept on the file and a copy provided to the person concerned. | SECURE DISPOSAL |
| Disciplinary Proceedings<br>Oral Warning<br>Written Warning 1<br>Written warning 2<br>Final Warning<br>Case not found | Yes | | | SECURE DISPOSAL<br>If warnings are placed on personal files, then they must be weeded from the file. |
| **HEALTH AND SAFETY** | | | | SECURE DISPOSAL |
| Health and Safety Policy Statements | No | | Life of policy plus 3 years. | SECURE DISPOSAL |

| Record Description | Data Protection Issues | Statutory Provisions | Retention information/period | Action at end of administrative life of the record (method of disposal) |
|---|---|---|---|---|
| Healthy and Safety risk Assessments | No | | Life of risk assessment plus 3 years. | SECURE DISPOSAL |
| Records relating to accident/injury at work | Yes | | | SECURE DISPOSAL |
| Accident Reporting<br>Adults<br>Students | Yes | Social Security (Claims and Payments) Regulations 1979 Regulation 25. Social Administration Act 1992 Section 8. Limitation Act 1980 | Date of incident plus 6 years.<br>Date of Birth of the student plus 25 years. | SECURE DISPOSAL |
| Control of Substances<br>Hazardous to Health (COSHH) | No | Control of substances Hazardous to Health Regulations 2002 SI2002 No 2677 Regulation 11; Records kept under 1994 and 1999 Regulations to be kept as if the 2002 Regulations had not been made. Regulation 18(2) | Current year plus 40 years. | SECURE DISPOSAL |
| Fire Log Book | No | | Current year plus 6 years. | SECURE DISPOSAL |
| **PAYROLL AND PENSIONS** | | | | |
| Maternity pay records | Yes | Statutory Maternity Pay (General) Regulations | Current year plus 3 years. | SECURE DISPOSAL |

| Record Description | Data Protection Issues | Statutory Provisions | Retention information/period | Action at end of administrative life of the record (method of disposal) |
|---|---|---|---|---|
| | | 1986 (SI1986/1960) revised 1999 (SI1999/567) | | |
| Records held under Retirement Benefits Schemes (Information Powers) Regulations 1995 | Yes | | Current year plus 6 years. | SECURE DISPOSAL |
| **RISK MANAGEMENT AND INSURANCE** | | | | |
| Employer's Liability Insurance Certificate | No | | Closure of the school plus 40 years. | SECURE DISPOSAL |
| **ACCOUNTS AND STATEMENTS INCLYDING BUDGET MANAGEMENT** | | | | |
| Annual Accounts | No | | Current year plus 6 years. | SECURE DISPOSAL |
| Loans and Grants managed by the school | No | | Date of last payment on the loan plus 12 years then REVIEW. | SECURE DISPOSAL |
| Student Grant applications | Yes | | Current year plus 3 years. | SECURE DISPOSAL |
| All records relating to the creation and management of budgets including the Annual Budget statement and background papers | No | | Life of the budget plus 3 years. | SECURE DISPOSAL |

| Record Description | Data Protection Issues | Statutory Provisions | Retention information/period | Action at end of administrative life of the record (method of disposal) |
|---|---|---|---|---|
| Invoices, receipts, order books and requisitions, delivery notices | No | | Current financial year plus 6 years. | SECURE DISPOSAL |
| Records relating to the collection and banking of monies | No | | Current financial year plus 6 years. | SECURE DISPOSAL |
| Records relating to the identification and collection of debt | No | | Current financial year plus 6 years. | SECURE DISPOSAL |
| **SCHOOL FUND** | | | | |
| School Fund – Cheque books | No | | Current financial year plus 6 years. | SECURE DISPOSAL |
| School Fund – Paying in books | No | | Current financial year plus 6 years. | SECURE DISPOSAL |
| School Fund - Ledger | No | | Current financial year plus 6 years. | SECURE DISPOSAL |
| School Fund - Invoices | No | | Current financial year plus 6 years. | SECURE DISPOSAL |
| School Fund - Receipts | No | | Current financial year plus 6 years. | SECURE DISPOSAL |
| School Fund – Bank Statements | No | | Current financial year plus 6 years. | SECURE DISPOSAL |
| **PROPERTY MANAGEMENT** | | | | |

| Record Description | Data Protection Issues | Statutory Provisions | Retention information/period | Action at end of administrative life of the record (method of disposal) |
|---|---|---|---|---|
| Leases of property leased by or to the school | No | | Expire of lease plus 6 years. | SECURE DISPOSAL |
| Records relating to the letting of school premises | No | | Current financial year plus 6 years. | SECURE DISPOSAL |
| **MAINTENANCE** | | | | |
| All records relating to the maintenance of the school carried out by contractors | No | | Current financial year plus 6 years. | SECURE DISPOSAL |
| **STUDENT'S EDUCATIONAL RECORD** | | | | |
| Students Educational Record required by The Education (Pupil Information) (England) Regulations 2005 | Yes | The Education (Pupil Information) (England) Regulations 2005 SI 2005 No. 1437<br>Limitation Act 1980<br>(Section 2) | Date of Birth of the student plus 25 years. | SECURE DISPOSAL |
| Examination Results | Yes | | This information should be added to the student file. | SECURE DISPOSAL |
| Child Protection information held on student's file | Yes | "Keeping children safe in education for schools and colleges"<br>"Working together to safeguard children. A guide to inter-agency | If any records relating to children protection issues are place on the student's file, it should be in a sealed envelope and then retained | SECURE DISPOSAL |

| Record Description | Data Protection Issues | Statutory Provisions | Retention information/period | Action at end of administrative life of the record (method of disposal) |
|---|---|---|---|---|
| | | working to safeguard and promote the welfare of children" | for the same period of time as the student's file. | |
| Child Protection information held in separate files | Yes | "Keeping children safe in education for schools and colleges"<br>"Working together to safeguard children. A guide to inter-agency working to safeguard and promote the welfare of children" | Date of Birth of the student plus 25 years then REVIEW – this retention period was agreed in consultation with the Safeguarding Children Group on the understanding that the principal copy of this information will be found on the Local Authority Social Services records. | SECURE DISPOSAL |
| **ATTENDANCE** | | | | |
| Attendance Registers | Yes | School attendance: Departmental advice for maintained schools, academies, independent schools and local authorities October 2014 | Every entry in attendance register must be preserved for a period of 3 years after the date on which the entry was made. | SECURE DISPOSAL |
| Correspondence relating to authorised absence | | Education Act 1996 Section 7 | Current academic year plus 2 years. | SECURE DISPOSAL |
| **SPECIAL EDUCATIONAL NEEDS** | | | | |

| Record Description | Data Protection Issues | Statutory Provisions | Retention information/period | Action at end of administrative life of the record (method of disposal) |
|---|---|---|---|---|
| Special Educational Needs files, reviews and Individual Education Plans | | Limitation Act 1980 Section 2 | Date of Birth of the student plus 25 years. | SECURE DISPOSAL |
| Advice and information provided to parents regarding educational needs | Yes | Special Educational Needs and Disability Act 2001 Section 2 | Date of Birth of the student plus 25 years (This would normally be retained on the student's file). | SECURE DISPOSAL unless the document is subject to a legal hold. |
| Accessibility Strategy | Yes | Special Educational Needs and Disability Act 2001 Section 14 | Date of Birth of the student plus 25 years (This would normally be retained on the student's file). | SECURE DISPOSAL unless the document is subject to a legal hold. |
| **STATISTICS AND MANAGEMENT INFORMATION** | | | | |
| Curriculum returns | No | | Current year plus 3 years. | SECURE DISPOSAL |
| Examination Results (Schools Copy)<br>Results<br><br><br>Examination Papers | Yes | | Current year plus 6 years.<br>Results recorded on the student's educational file will be retained until the student reaches the age of 25 years.<br>The examination papers should be kept until any appeals/validation process is complete | SECURE DISPOSAL |
| Published Admission Number (PAN) Reports | Yes | | Current year plus 6 years. | SECURE DISPOSAL |

| Record Description | Data Protection Issues | Statutory Provisions | Retention information/period | Action at end of administrative life of the record (method of disposal) |
|---|---|---|---|---|
| | | | | |
| **IMPLEMENTATION OF CURRICULUM** | | | | |
| Schemes of Work | No | | Current year plus 1 year. | SECURE DISPOSAL |
| Timetable | No | | Current year plus 1 year. | SECURE DISPOSAL |
| Marks | No | | Current year plus 1 year. | SECURE DISPOSAL |
| Record of Homework Set | No | | Current year plus 1 year. | SECURE DISPOSAL |
| Student's Work | No | | Current year plus 1 year. | SECURE DISPOSAL |
| **EXTRA CURRICULAR ACTIVITIES** | | | | |
| Parental consent forms for school trips where there has been no major incident | Yes | | Conclusion of the trip. | SECURE DISPOSAL |
| Parental permission slips for school trips – where there has been a major incident | Yes | Limitation Act 1980<br>Section 2 | Date of Birth of the student involved plus 25 years. The permission slips for all the students on the trip need to be retained to show that the rules had been followed for all students. | SECURE DISPOSAL |
| **LOCAL AUTHORITY** | | | | |

| Record Description | Data Protection Issues | Statutory Provisions | Retention information/period | Action at end of administrative life of the record (method of disposal) |
|---|---|---|---|---|
| Attendance Returns | Yes | | Current year plus 2 years. | SECURE DISPOSAL |
| School Census Returns | No | | Current year plus 5 years. | SECURE DISPOSAL |
| Circulars and other information sent from the Local Authority | No | | Operational use. | SECURE DISPOSAL |
| **CENTRAL GOVERNMENT** | | | | |
| OFSTED/Other Regulatory Reports and Papers | No | | Life of the report then REVIEW. | SECURE DISPOSAL |
| Returns made to central government | No | | Current year plus 6 years. | SECURE DISPOSAL |
| Circular and other information sent from central government | No | | Operational use. | SECURE DISPOSAL |