**General Data Protection Regulation (GDPR) Policy**
**Incorporating Freedom of Information**

**Document Control Information**

| Version | DATE | DESCRIPTION |
|---|---|---|
| 7 | 10/06/2020 | Minor amendments. Change responsibility to Tom Scantlebury. |
| 8 | 16/06/2021 | Reviewed with no changes |
| 9 | 04/05/2022 | Removal of repeated statements, processes and streamline statements to be specific. New links to ICO website |
| 10 | 15/06/2023 | Reviewed with minor change |
| 11 | 02/07/2024 | Complete update due to changes in law and guidance |
| 12 | 10/03/2025 | Reviewed with no changes |

| | |
|---|---|
| Reviewed | 10/03/2025 |
| Responsibility | Iain Thomas |
| Committee | FMC |
| Review Date | March 2026 |
| Signed | |

1. Scope
   a. Foundry College is committed to protecting all data that it holds relating to staff, pupils, parents and members of the Management Committee.

   b. This policy applies to the storing of all college data regardless of whether it is in paper, electronic, photographic or videographic format.

2. Legislation and guidance

This policy meets the requirements of the Data Protection Act 2018 (which incorporates the General Data Protection Regulations 2020) and is based on guidance published by the Information Commissioner's Office (ICO) and the Department for Education (DFE). It also reflects the ICO's guidance 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. Data protection principles and categories of data
   a. The Data Protection Act 2018 sets out six data protection principles that the college must follow when processing personal data. Data must be:
      - Processed fairly, lawfully and in a transparent manner
      - Used for specified, explicit and legitimate purposes
      - Used in a way that is adequate, relevant and limited to only what is necessary
      - Accurate and, where necessary, kept up-to-date
      - Kept no longer than is necessary
      - Processed in a manner that ensures appropriate security of the data

   b. Categories and definitions of data
      i. The Data Protection Act 2018 refers to **Personal data** and **Special categories of personal data**
         - **Personal data** means any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier.
         - **Special categories of personal data** (previously known as 'sensitive personal data') includes race, ethnic origin, politics, religion, trade union membership, genetics, biometrics, health and sexual orientation.

      ii. Note that the DfE consider it best practice that data such as free school meal status, pupil premium eligibility, elements of special educational need, safeguarding, some behaviour data and Children's Services interactions are also treated with the same care as the special categories set out in law.

| TERM | DEFINITION |
|---|---|
| **Personal data** | Any information relating to an identified, or identifiable, living 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. |

| TERM | DEFINITION |
|---|---|
| **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 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. Roles and responsibilities

a. College staff and The Management Committee have a duty to comply with this policy. (All staff and members of The Management Committee should note that the Data Protection Act 2018 makes provision for significant fines to be levied in the event of non-compliance.)

b. The Data Controller is the competent authority which, alone or jointly with others determines the purpose and means of processing personal data.

c. Data Protection Officer acts as the contact point for all Data Protection issues and queries from Data Subjects and the ICO, e.g. for Subject Access Requests and data breaches.

d. Data processor will ensure that all third parties are compliant with the Data Protection Act 2018.

## 5. Data Protection documentation

a. Privacy Notices
   i. The college will make available Privacy Notices via the college website.

b. Consent

i. Where required, the college will seek and record specific consent from data subjects (e.g. image permissions, email marketing, biometrics).

## 6. Data protection principles

The UK 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 we aim to comply with these principles.

## 7. Collecting personal data

### 7.1 Lawfulness, fairness and transparency

We will only process personal data where we have 1 of 6 'lawful bases' (legal reasons) to do so under data protection law:

- The data needs to be processed so that the school can **fulfil a contract** with the individual, or the individual has asked the school to take specific steps before entering into a contract
- The data needs to be processed so that we 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 Foundry College, 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 Foundry College (where the processing is not for any tasks that we perform as a public authority) or a third party, provided the individual's rights and freedoms are not overridden
- The individual (or their parent/carer when appropriate in the case of a pupil) has freely given clear **consent**

For special categories of personal data, we will also meet 1 of the special category conditions for processing under data protection law:

- The individual (or their parent/carer when appropriate in the case of a pupil) 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 when appropriate in the case of a pupil) 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 our 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 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 that can provide sufficient guarantees that they comply with UK 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 situation that affects any of our pupils or staff.

Where we transfer personal data internationally, we will do so in accordance with UK 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 Foundry College 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
- 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, most subject access requests from parents or carers of pupils at Foundry College 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.

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

### 9.3 Responding to subject access requests

When responding to requests, we:

- 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 (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 3 months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within 1 month, and explain why the extension is necessary

We 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 pupil 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 can't reasonably anonymise, and we don't 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 that 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. Parental requests to see the educational record

Parents, or those with parental responsibility, have a legal right to free access to their child's educational record (which includes most information about a pupil) within 15 school days of receipt of a written request.

If the request is for a copy of the educational record, we may charge a fee to cover the cost of supplying it.

This right applies as long as the pupil concerned is aged under 18.

There are certain circumstances in which this right can be denied, such as if releasing the information might cause serious harm to the physical or mental health of the pupil or another individual, or if it would mean releasing exam marks before they are officially announced.

## 11. CCTV

We use CCTV in various locations around the site to ensure it remains safe. We will follow the ICO's guidance for the use of CCTV, and comply with data protection principles.

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 Iain Thomas, Headteacher.

## 12. Photographs and videos

As part of our daily 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 the pupil.

Any photographs and videos taken by parents/carers at school events for their own personal use are not covered by data protection legislation. However, we will ask that photos or videos with other pupils are not shared publicly on social media for safeguarding reasons, unless all the relevant parents/carers have agreed to this.

Where Foundry College takes photographs and videos, uses may include:

- Within the premises on notice boards and in brochures, newsletters, etc.
- Outside by external agencies such as the school 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.

## 13. Artificial intelligence (AI)

Artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Bard.

Foundry College recognises that AI has many uses to help pupils learn, but also poses risks to sensitive and personal data.

To ensure that personal and sensitive data remains secure, no one will be permitted to enter such data into unauthorised generative AI tools or chatbots.

If personal and/or sensitive data is entered into an unauthorised generative AI toolFoundry College will treat this as a data breach, and will follow the personal data breach procedure outlined in appendix 1.

## 14. Data protection by design and default

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

- Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge
- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law (see section 6)
- Completing data protection impact assessments where the school's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on this process)
- Integrating data protection into internal documents including this policy, any related policies and privacy notices
- Regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters; we will also keep a record of attendance
- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant
- Appropriate safeguards being put in place if we transfer any personal data outside of the UK, where different data protection laws may apply
- Maintaining records of our processing activities, including:
    - For the benefit of data subjects, making available the name and contact details of our college 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 UK and the safeguards for those, retention periods and how we are keeping the data secure

## 15. Data security and storage of records

We will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage.

In particular:

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data, are kept under lock and key when not in use
- Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, or left anywhere else where there is general access
- Where personal information needs to be taken off site, staff must sign it in and out from the admin office

- Passwords that are at least 10 characters long containing letters and numbers are used to access school computers, laptops and other electronic devices. Staff and pupils are reminded that they should not reuse passwords from other sites
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices
- Staff, pupils or governors who store personal information on their personal devices are expected to follow the same security procedures as for school-owned equipment (see our [online safety policy / ICT policy / acceptable use agreement / policy on acceptable use])
- Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected (see section 8)

**16. 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.

**17. Personal data breaches**

Foundry College 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 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

**18. 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.

**19. Monitoring arrangements**

The DPO is responsible for monitoring and reviewing this policy.

This policy will be reviewed annually and approved by the full governing board.

7. This policy should be read in conjunction with all Foundry College policies

8. If you would like to contact the Foundry College Data Protection Officer (DPO):

   Email: DPO@foundry.wokingham.sch.uk
   Or by post:
   Data Protection Officer

Foundry College
Budges Gardens
Wokingham
RG40 1PX
01183341510

**APPENDIX 1**

**(a) Data breach information and procedures**

Data protection breaches can be caused by a number of factors, e.g. Loss or theft of pupil, staff or Management Committee data and/or equipment or paperwork on which data is stored, inappropriate access controls allowing unauthorised use, poor data destruction procedures, human error such as sending an email to the wrong person, cyber-attack, hacking, ransom ware.

In the event of a breach, the procedures below should be followed:

1. Any data protection incident should be reported immediately to the college's DPO and Headteacher.

2. If required, appropriate actions should be taken to halt the breach, and/or prevent further breaches.

3. The DPO must report any significant data protection incidents to the ICO within 72 hours of the breach being detected, where feasible.

4. The Chair of the Management Committee should be informed as soon as possible. Other agencies as appropriate may need to be informed depending on the breach, e.g. police, Action Fraud, social services.

5. Where the breach involves the disclosure of the personal data of specific individuals, they should usually be notified.

6. Fully investigate the breach, and review all related policies and procedures to make any necessary changes.

7. Provide additional training to staff as appropriate.

8. Review whether any disciplinary action should be taken.

9. If the nature of the breach could result in adverse publicity the college may wish to prepare a statement for publication.

10. A full record should be kept of all data breaches, including all the steps taken, whether reportable or not.

**Additional notes**

In the event of a data breach, the following areas will need to be considered:

- The type of data and its sensitivity
- What protections were in place (e.g. encryption)
- What has happened to the data
- Whether the data could be put to any illegal or inappropriate use
- How many people are affected
- What type of people have been affected (pupils, staff members, suppliers etc.) and whether there are wider consequences to the breach.

## (b) Subject Access Request (SAR) Process and Timescales

A SAR is a request for personal data about the applicant.
The format a SARs can be made;

- Verbally – followed up with written confirmation
- Letter
- Email

1. Clarify that this is a SAR and not some other request for information, i.e. a FOI request or an 'educational record' request.

2. Confirm the identity of the person making the request.

3. If it is unclear what information is being requested, ask for further details from the applicant.

4. Check that the information is available:
   - If the information is not available, inform the applicant.
   - If the information is available, note the date that the SAR was received or, in the case of further details being requested, the date that these were received. The college now has one calendar month to respond.

5. Check whether the information requested contains information about any third-party. If it does then undertake one, or more, of the following steps:
   - Seek permission to disclose the information from the third-party concerned.
   - Redact/summarise the information to protect the identity of the third-party.
   - Withhold the information to protect the rights of the third-party.

6. Ensure that the information to be supplied is clear and understandable, e.g. any complex codes or terms are explained.

7. Supply the information requested in an appropriate format, e.g. if the request is made electronically, the information should be provided in an electronic format.

8. Keep a record of the SAR and any information that was supplied.

## (c) Freedom of Information (FOI) Process and Timescales

A FOI request may be made by any member of the general public, as they have a right to know about the activities of public authorities, which includes schools. The college will normally disclose the information requested in whole or part unless there is a clear and accepted reason not to do so.

All FOI requests must be in writing, either paper or electronic, and must contain the applicant's contact details. All requests should be directed to the DPO.

### Additional Notes

- More information can be found on the Information Commissioners office website Home | ICO
- The college may charge for the cost of copying and postage, where appropriate.
- The college may refuse an entire request under various circumstances.

**APPENDIX 2**

The following retention guidelines are for data that has a possible risk of becoming a Data Protection issue.

| Document | Retention Period | Disposal Method |
|---|---|---|
| Records relating to complaints dealt with by the Management Committee | 6 years from date of resolution | Review that issue is not still contentious then secure disposal |
| Professional Development plans | Closure of the plan plus 6 years | Secure disposal |
| Admissions (if successful) | Date of admission plus 1 year | Secure disposal |
| Register of Admissions | Date of last entry plus 6 years | Review and may be kept permanently |
| Proofs of address supplied by parent as part of admissions process | Current year plus 1 year | Secure disposal |
| Supplementary information form including additional information such as religion, medical conditions | Current year plus 1 year | Secure disposal |
| Visitors books & signing in sheets | Current year plus 2 years then review | Secure disposal |
| All records leading up to the appointment of a Headteacher | Date of appointment plus 6 years | Secure disposal |
| All records leading up to the appointment unsuccessful staff applicants | Date of appointment of successful candidate + 6 months | Secure disposal |
| All records leading up to the successful applicant appointment that do not form part of their Staff Personnel file | 6 months | Secure disposal |
| DBS checks | Should NOT be kept for more than 6 months | Secure disposal |
| Staff Personnel file | Termination date + 7 years | Secure disposal |
| Timesheets | Current year + 6 years | Secure disposal |
| Appraisal | Current year + 5 years | Secure disposal |
| Disciplinary proceedings<br>Oral warning<br>Written warning level 1<br>Written warning level 2<br>Final warning<br>Case not found | Date of warning + 6 months<br>Date of warning + 6 months<br>Date of warning + 12 months<br>Date of warning + 18 months<br>No record<br>Unless a child protection issue, dispose of documents at conclusion of the case. If child protection keep for either 10 years or until retirement whichever is the longer | Secure disposal |

| | | |
|---|---|---|
| Records relating to accident / injury at work | Date of incident plus 12 years | Secure disposal |
| Maternity Pay records | Current Year plus 6 years | Secure disposal |
| FSM Registers | Current year plus 6 years | Secure disposal |
| School Meal Registers | Current year plus 6 years | Secure disposal |
| Pupils Education Record | DoB plus 25 years | Secure disposal |
| Child Protection info held on pupil file | Held in a sealed envelope for the same period of time as the file | These MUST be shredded |
| CP info held on separate files | DoB plus 25 years then REVIEW | These MUST be shredded |
| Attendance Registers | Date of entry plus 6 years | Secure disposal |
| Authorised absence correspondence | Current academic year plus 2 years | Secure disposal |
| SEND files , reviews, IEP's statements, advice and information provided to parents, accessibility strategy | Pupil DoB plus 25 years | Secure disposal |
| Examination Results | Current year plus 6 years | Secure disposal |