



# Walkwood

Church of England  Middle School

## Data Protection Policy

Governing Body Committee responsible:	Full board		
Approval granted:	11 July 2022	Review date:	Summer Term 2024

“Don’t try to be mean to neighbours who trust you. Don’t argue just to be arguing, when you haven’t been hurt. Don’t be jealous of cruel people or follow their example.”

*Proverbs 3: 29-31*

“Church of England Schools have at their heart a belief that all children are loved by God, are individually unique and that the school has a mission to help each pupil to fulfil their potential in all aspects of their personhood: physically, academically, socially, morally and spiritually. Schools have a duty to try to remove any factor that might represent a hindrance to a child’s fulfilment. We want all pupils to want to engage in learning in a safe and welcoming ethos.”

*Valuing All God’s Children, Church of England, 2014*

“The core purpose of any Church school is to maximise the learning potential of every pupil within the love of God.”

*SIAMS (Statutory Inspection of Anglican and Methodist Schools) 2012*



## Aims

Our school aims to ensure that all personal data collected about staff, pupils, parents, governors, visitors and other individuals is collected, stored and processed in accordance with the United Kingdom's General Data Protection Regulation and the corresponding legislation, the Data Protection Act 2018.

This policy applies to all personal data, regardless of whether it is in paper or electronic format.

## Legislation and guidance

This policy meets the requirements of the United Kingdom's General Data Protection Regulation and the corresponding legislation, the Data Protection Act 2018. It is based on guidance published by the Information Commissioner's Office on the United Kingdom's General Data Protection Regulation and the Information Commissioner's Office's code of practice for subject access requests.

It meets the requirements of the Protection of Freedoms Act 2012 when referring to our use of biometric data.

It also reflects the Information Commissioner's Office's Code of Practice for the use of surveillance cameras and personal information.

In addition, this policy complies with our funding agreement and articles of association.

## Definitions

Term	Definition
<b>Personal data</b>	<p>Any information relating to an identified, or identifiable, individual. This may include the individual's:</p> <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> <p>It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.</p>
<b>Special categories of personal data</b>	<p>Personal data which is more sensitive and so needs more protection, including information about an individual's:</p> <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</li><li>• Health – physical or mental</li></ul>



	<ul style="list-style-type: none"> <li>• Sex life or sexual orientation</li> </ul>
<b>Processing</b>	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.
<b>Data subject</b>	The identified or identifiable individual whose personal data is held or processed.
<b>Data controller</b>	A person or organisation that determines the purposes and the means of processing of personal data.
<b>Data processor</b>	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.
<b>Personal data breach</b>	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

## The data controller

Our school processes personal data relating to parents, pupils, staff, governors, visitors and others, and therefore is a data controller.

The Walkwood Academy Trust (of which the school is the sole organisation) is registered as a data controller with the Information Commissioner's Office and will renew this registration annually or as otherwise legally required.

## Roles and responsibilities

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

### Governing body

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

### Data protection officer

The Data Protection Officer 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 Data Protection Officer is also the first point of contact for individuals whose data the school processes, and for the Information Commissioner's Office.



Our Data Protection Officer is contactable via [office@walkwoodms.worcs.sch.uk](mailto:office@walkwoodms.worcs.sch.uk), stating 'Data Protection Officer' in the subject line.

### Principal

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

### All staff

Staff are responsible for:

- collecting, storing and processing any personal data in accordance with this policy;
- informing the school of any changes to their personal data, such as a change of address;
- contacting the Data Protection Officer in the following circumstances -
  - with any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure;
  - if they have any concerns that this policy is not being followed;
  - if they are unsure whether or not they have a lawful basis to use personal data in a particular way;
- if they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the European Economic Area;
- if there has been a data breach;
- whenever they are engaging in a new activity that may affect the privacy rights of individuals;
- if they need help with any contracts or sharing personal data with third parties.

## Data protection principles

The United Kingdom's General Data Protection Regulation and the corresponding legislation, the Data Protection Act 2018, is based on data protection principles that our school must comply with.

The principles say that personal data must be:

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

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

## Collecting personal data

### Lawfulness, fairness and transparency

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



- The data needs to be processed so that the school can **fulfil a contract** with the individual, or the individual has asked the school to take specific steps before entering into a contract.
- The data needs to be processed so that the school can **comply with a legal obligation**.
- The data needs to be processed to ensure the **vital interests** of the individual e.g. to protect someone's life.
- The data needs to be processed so that the school, as a public authority, can perform a task **in the public interest**, and carry out its official functions.
- The data needs to be processed for the **legitimate interests** of the school or a third party (provided the individual's rights and freedoms are not overridden).
- The individual (or their parent/carer when appropriate in the case of a 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 United Kingdom's General Data Protection Regulation and the corresponding legislation, the Data Protection Act 2018.

If we offer online services to pupils, such as classroom apps, and we intend to rely on consent as a basis for processing, we will get parental consent where the pupil is under 13 (except for online counselling and preventive services). For pupils in Year 8, we shall seek their own consent.

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

### Limitation, minimisation and accuracy

We will only collect personal data for specified, explicit and legitimate reasons. We will explain these reasons to the individuals when we first collect their data.

If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so, and seek consent where necessary.

Staff must only process personal data where it is necessary in order to do their jobs. When staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. Personal data will be deleted by 12 months after a pupil's year group has left the school.

## Sharing personal data

We will not normally share personal data with anyone else, but may do so where:

- there is an issue with a pupil or parent/carer that puts the safety of our staff at risk;
- we need to liaise with other agencies – we will seek consent as necessary before doing this;
- our suppliers or contractors need data to enable us to provide services to our staff and pupils – for example, Lourdes IT. When doing this, we will:
  - only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law;



- establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data we share;
- only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us.

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

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

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

Where we transfer personal data to a country or territory outside the European Economic Area, we will do so in accordance with data protection law.

## Subject access requests and other rights of individuals

### 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 must be submitted in writing, to the Data Protection Officer. They should include:

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

We are able to provide a form if that is more helpful.



If staff receive a subject access request they must immediately forward it to the Data Protection Officer.

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

Children aged 13 and above are generally regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of pupils at our school 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.

### 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. 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 takes into account administrative costs.

A request will be deemed to be unfounded or excessive (refers to information about more than one academic year), if it is repetitive (refers to more than 3 requests in an academic year), or asks for further copies of the same information.

When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the Information Commissioner's Office.

### Other data protection rights of the individual





In addition to the right to make a subject access request (see above), and to receive information when we are collecting their data about how we use and process it (see section 7), individuals also have the right to:

- withdraw their consent to processing at any time;
- ask us to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances);
- prevent use of their personal data for direct marketing;
- challenge processing which has been justified on the basis of public interest;
- request a copy of agreements under which their personal data is transferred outside of the European Economic Area;
- object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them);
- prevent processing that is likely to cause damage or distress;
- be notified of a data breach in certain circumstances;
- make a complaint to the Information Commissioner's Office;
- 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 Data Protection Officer. If staff receive such a request, they must immediately forward it to the Data Protection Officer.

## Parental requests to see the educational record

Walkwood Church of England Middle School is an academy with deeds and articles from the Department for Education. In academies, there is no automatic parental right of access to the educational record. If copies of the annual school report are required, these may be applied for by contacting the Data Protection Officer using [office@walkwoodms.worcs.sch.uk](mailto:office@walkwoodms.worcs.sch.uk), stating 'Data Protection Officer' in the subject line.

## Biometric recognition systems

Where we use pupils' biometric data as part of an automated biometric recognition system (for example, pupils use finger prints to receive school lunches instead of paying with cash), we will comply with the requirements of the Protection of Freedoms Act 2012.

Parents/carers will be notified before their child first takes part in it. Such information is supplied within the Pupil Data Collection booklet. The school will get written consent from at least one parent or carer before we take any biometric data from their child and first process it.

Parents/carers and pupils have the right to choose not to use the school's biometric system(s). We will provide a Personal Identification Number (PIN) for those pupils.

Parents/carers and pupils can object to participation in the school's biometric recognition system(s), or withdraw consent, at any time, and we will make sure that any relevant data already captured is deleted.

As required by law, if a pupil refuses to participate in, or continue to participate in, the processing of their biometric data, we will not process that data irrespective of any consent given by the pupil's parent(s)/carer(s).

Where staff members or other adults use the school's biometric system(s), we will also obtain their consent before they first take part in it, and provide alternative means of accessing the relevant service if they object. Staff and other adults can also withdraw consent at any time, and the school will delete any relevant data already captured.

## CCTV

We use CCTV in various locations around the school site to ensure it remains safe. We refer to the Information Commissioner's Office's Code of Practice for the use of CCTV.

We do not need to ask individuals' permission to use CCTV: we are carrying out a legal obligation for the safety of staff and pupils, and ensuring that policies are adhered to as part of the convention that exists between pupils, parents and the school, along with the obligations between employer and employee. CCTV is intended to ensure safety, security and supervision.

CCTV images may be used where there is good cause to suspect that an illegal or unauthorised action(s) is taking place, or where there are grounds to suspect misconduct.

We make it clear that individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs at entrances explaining that CCTV is in use. Images are retained for 19 days, thus allowing any matter that requires the use of CCTV images to be instigated and investigated. Data is erased after this time.

Access to CCTV images is restricted to members of the senior leadership team, college leaders and pastoral managers, the site manager and business manager. The conduct of pupils around the site may require that images are retained because of a particular incident. Regarding staff, CCTV will not be used to gather data for performance appraisal purposes or in capability procedures, and in any other circumstances, CCTV will only be viewed by members of the senior leadership team.

## Photographs and videos

As part of our school activities, we may take photographs and record images of individuals within our school. Images may be used internally to allow us to work effectively as a school.

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

Uses may include:

- within school on notice boards, the prospectus and The Insider;
- outside of school by external agencies such as the school photographer or a newspapers;
- online on our school website or Twitter.



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.

If we make use of photographs for staff use to aid the running of the school, such as to identify pupils within a tutor group or who have medical needs, these shall be displayed in the staff area where there is controlled access.

## 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 Data Protection Officer, 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 'Data protection principles' on page 5);
- 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 Data Protection Officer will advise on this process);
- integrating data protection into internal documents including this policy, any related policies and privacy notices;
- regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters - we will also keep a record of attendance;
- regularly conducting reviews and audits to test our privacy measures and make sure we are compliant;
- maintaining records of our processing activities, including:
  - for the benefit of data subjects, making available the name and contact details of our school and Data Protection Officer 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.

## 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.

- 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
- Where personal information needs to be taken off site, staff must sign it in and out from the school office
- Passwords that are at least 8 characters long containing letters and numbers are used to access school computers, laptops and other electronic devices. Staff and pupils are reminded to change their passwords at regular intervals
- Encryption software is used to protect all portable devices and removable media, such as laptops
- Staff, pupils or governors who store personal information on their personal devices are expected to follow the same security procedures as for school-owned equipment (see our acceptable use policy)
- Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected (see 'Sharing personal data' on page 7)

As far as possible, personal data will be kept in an electronic format on a server that staff can access remotely when working from home. Ensuring this data is stored remotely means it cannot be misplaced or lost.

Documents with little personal data, such as pupils' work books or assessed work, are suitably low risk that they may be taken home by staff. This is also practical, as it allows teachers to mark work more flexibly.

## Retention of records

Personal data will be retained up to 12 months after a pupil's year group has left the school. However, there may be situations where the law requires us to hold the data for longer. If there has been a significant accident, then we shall hold that information for five years after the pupil has left the school.

When a pupil leaves the school to move to their next educational provider, all relevant personal data and the pupil's educational record, including any safeguarding information, will be securely passed to the receiving setting.

Staff information will be retained for five years after their employment has ceased.

## 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.

## Personal data breaches

The school will make all reasonable endeavours to ensure that there are no personal data breaches. In the unlikely event of a suspected data breach, we will follow the procedure set out in appendix 1.

When appropriate, we will report the data breach to the Information Commissioner's Office 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.

## 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.

## Monitoring arrangements

The Data Protection Officer is responsible for monitoring and reviewing this policy.

This policy will be reviewed and updated if necessary when the Data Protection Bill receives royal assent and becomes law (as the Data Protection Act 2018) – if any changes are made to the bill that affect our school's practice. Otherwise, or from then on, this policy will be reviewed **every 2 years** and shared with the full governing board.



## Appendix 1: Personal data breach procedure

This procedure is based on guidance on personal data breaches produced by the Information Commissioner's Office.

- On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the Data Protection Officer
- The Data Protection Officer will investigate the report, and determine whether a breach has occurred. To decide, the Data Protection Officer 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 Data Protection Officer will alert the Principal and the Chair of Governors
- The Data Protection Officer 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 Data Protection Officer will assess the potential consequences, based on how serious they are, and how likely they are to happen
- The Data Protection Officer will work out whether the breach must be reported to the Information Commissioner's Office. This must be judged on a case-by-case basis. To decide, the Data Protection Officer will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:
  - Loss of control over their data
  - Discrimination
  - Identify theft or fraud
  - Financial loss
  - Unauthorised reversal of pseudonymisation (for example, key-coding)
  - Damage to reputation
  - Loss of confidentiality
  - Any other significant economic or social disadvantage to the individual(s) concerned
  - If it's likely that there will be a risk to people's rights and freedoms, the Data Protection Officer must notify the Information Commissioner's Office.
- The Data Protection Officer will document the decision (either way), in case it is challenged at a later date by the Information Commissioner's Office or an individual affected breach.



- Where the Information Commissioner’s Office must be notified, the Data Protection Officer will do this via the ‘report a breach’ page of the Information Commissioner’s Office website within 72 hours. As required, the Data Protection Officer 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 Data Protection Officer
  - 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 Data Protection Officer 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 Data Protection Officer expects to have further information. The Data Protection Officer will submit the remaining information as soon as possible
- The Data Protection Officer 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 Data Protection Officer will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:
  - The name and contact details of the Data Protection Officer
  - A description of the likely consequences of the personal data breach
  - A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned
- The Data Protection Officer 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 Data Protection Officer will document each breach, irrespective of whether it is reported to the Information Commissioner’s Office. For each breach, this record will include the:
  - Facts and cause
  - Effects
  - Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)
  - Records of all breaches will be stored electronically.
- The Data Protection Officer and Principal 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 (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error
- Members of staff who receive personal data sent in error must alert the sender and the Data Protection Officer as soon as they become aware of the error
- If the sender is unavailable or cannot recall the email for any reason, the Data Protection Officer will ask the ICT department to recall it
- In any cases where the recall is unsuccessful, the Data Protection Officer 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 Data Protection Officer will ensure we receive a written response from all the individuals who received the data, confirming that they have complied with this request
- The Data Protection Officer 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
- Details of pupil premium interventions for named children being published on the school website
- Non-anonymised pupil exam results or staff pay information being shared with governors
- A school laptop containing non-encrypted sensitive personal data being stolen or hacked
- The school's cashless payment provider being hacked and parents' financial details stolen





## Appendix 2: GDPR aide memoire

If something doesn't seem right, talk to our data protection officer (DPO) – Mrs S Hill

Report to our data protection officer immediately if you think personal data has been lost, stolen or wrongly disclosed. This is so we can quickly take steps to mitigate the impact of the breach.

You should also speak to our data protection officer if:

- You have any concerns at all about keeping personal data safe
- You're introducing a new process or policy that involves using personal data
- Anyone asks you to see the data that we have about them. This is called a 'subject access request', and the person will be entitled to this information

**Personal data:** any information relating to an identifiable living person, e.g. name, contact details, ID numbers, attendance and assessment information, financial information

**Sensitive personal data:** includes information that reveals someone's ethnic origin, political opinions, religion, sexuality or health. In our school, it also means safeguarding information, and whether a child is looked-after, has SEN, or is eligible for free school meals

### Do:

- ✓ **Remember that data protection laws DO NOT stop you from reporting safeguarding concerns**
  - You must still report to the relevant people where you're concerned about a child. You do not need anyone's consent to do this
- ✓ **Only collect the information you actually need**
  - When you're requesting information (for example, via consent forms, admissions forms or surveys) ask yourself "Do I really need this? What will I actually use it for?"
  - If you don't need it, or only want it "just in case", don't collect it
  - If you've already collected personal information that you don't need, delete it
- ✓ **Keep personal data anonymous, if possible**
  - For example, if you're emailing a colleague about accommodating a pupil's religion, or about managing a pupil's medical condition, don't name the child if you don't need to
  - This is particularly important with photographs for external use – if you have an image of a child, don't attach their name to it unless you have explicit consent to do so
- ✓ **Think before you put information up on the wall**
  - If your display is an essential part of teaching and learning, or helps to keep pupils safe, it's fine. This might include medical information, or a list of parents' evening appointments. Still only display the information you really need to
  - If your display is non-essential, promotional, or there might be a safeguarding risk, either ask the pupil or parents for consent first or just don't display it



- ✓ **Take care when you're taking personal information home with you**
  - Sign documents containing personal data out and in from the school office
  - Keep physical documents in a secure, closed folder along with your contact details in case the folder is lost
  - Store the documents in a safe place at home – don't leave them in your car or at a friend's house
  
- ✓ **Practise good ICT security**
  - Passwords should be at least 7 characters, with upper and lower-case letters and special characters
  - Password-protect documents and email attachments that include personal data
  - Always double-check that you're emailing personal data to the correct person, who is authorised to see it
  - Use 'bcc' when you're emailing a group of people who don't have email addresses for everyone else in the group, e.g. parents or volunteers

## Don't:

- ✗ **Leave personal data out on your desk**
  - Keep your desk clear, so people cannot see information about others accidentally. The same goes for personal data written on post-it notes, on top of the printer, or on an unattended computer screen
  
- ✗ **Take any sensitive personal information home with you**
  - If the information is confidential, sensitive or risky, it's best to leave it on the school site or computer system, where there are security measures and processes in place
  
- ✗ **Use memory sticks**



## Appendix 3: Personal data retention periods

Data item	Short term event +1 month	Medium term individual at school +1 year	Long term individual at school +5 years	Very long term pupil is aged 25 or older	Justification
Admissions		✓			Admissions data is used extensively from the period of the school receiving it up until the point where children enrol. Once enrolled, the child's records in SIMS become the core record. Data about children who enrolled but didn't get in is useful, but any intelligence gathered from it is aggregated within the first year to a level being non-personal. After that, the detailed data within the admission file can be deleted.
Attainment		✓	✓		Formative assessment data is useful as a child is building towards a particular more formal assessment. Once the child leaves the school, it has little value in terms of retention. Summative attainment is the main outcome of what children 'attain' in school. It is important that future schools where pupils go on to learn can understand previous attainment. Whilst often that information is 'passed on' smoothly as children move phase, it is not always the case, and thus retaining the names alongside the main attainment data for 1 year after the pupil has left the school feels proportionate. Trend analysis is important, 3 to 5 years is often the 'trend' people look at, but longer may be relevant. Whilst this must be fully flexible in reporting small sub groups, and the data would wish to be retained at individual level, some personal data (for example, name) could be removed from the data to reduce sensitivity. After 3 to 5 years, then aggregated summaries that have no risk of identifying individuals are all that are typically needed to be retained.



Data item	Short term event +1 month	Medium term individual at school +1 year	Long term individual at school +5 years	Very long term pupil is aged 25 or older	Justification
Attendance		✓			Attendance is related to individual attainment and so being able to relate attendance to attainment whilst in our care is important. Keeping it in detailed, individual form for one year after the pupil leaves school support conversations about detailed attendance that may be needed to best support that child. After that period, non-identifiable summary statistics are all that is required to support longer term trend analysis of attendance patterns.
Behaviour		✓			This is all relevant for managing children when with at your school. 1 year allows a period of 'handover' to next institution with conversations supported by rich data if relevant.
Catering and free school meal management		✓ (meal administration)	✓ (free school meal eligibility information)		A short historic record of what a child has had may be useful in case of any food-related incidents at school, or parental queries about the types of meals their children are choosing. Keeping for up to one year also allows time to do accounting work associated with catering. Typically 'one month' may not be enough, but 'one year' feels enough. Due to the way school funding works, free school meal eligibility is a financial matter, and thus keeping this data for 6+1 feels appropriate. This 7- year record also needs to be portable with the pupil, as historic dates can be used for funding.
Complaints		✓			Complaints that are part of the formal process, either stage 2 or 3 of the Complaints Policy, are held in school. Correspondence, information submitted as part of either stage, and records relating to individual complaints are to be kept confidential except where the Secretary of State or a body conducting an inspection under section 109 of the 2008 Act requests access to them.
Exclusions		✓			Exclusion data should be 'passed on' to subsequent settings. That school then has responsibility for retaining the full history of the child. If a private setting or the school is unsure on where the child has



Data item	Short term event +1 month	Medium term individual at school +1 year	Long term individual at school +5 years	Very long term pupil is aged 25 or older	Justification
					gone, then the school should ensure the LA already has the exclusion data.
Identity management and authentication		✓	✓		<p>While a pupil is at the school, we shall use the photographs with pupil names to aid identification.</p> <p>Once a pupil has left the school, we shall ensure their images are no longer linked to their names, and any pictures that are on the website are removed for school leavers.</p> <p>For special events, such as plays, sporting events or whole school photographs, these may continue to be displayed in school but no names will be attached to the images.</p>
Trips and visits	✓		✓ (financial information related to trips)	✓ (major medical events)	<p>Financial information related to trips should be retained for 6 years + 1 for audit purposes. This would include enough child identifiers to be able to confirm contributions.</p> <p>The information that is taken on a trip by school can be destroyed following the trip, once any medicines administered on the trip have been entered onto the core system. If there is a minor medical incident (for example, a medical incident dealt with by staff in the way it would be dealt with 'within school') on the trip, then adding it into the core system would be done.</p> <p>If there is a major incident (for example, a medical incident that needed outside agency) then retaining the entire file until time that the youngest child becomes 25 would be appropriate.</p> <p>Permission to go on the trip slips will contain personal data, and destroying them after the trip unless any significant incident arises is appropriate.</p> <p>We sometimes share personal data with people providing 'educational visits' into school. There should be good procedures in place to ensure that the sharing is proportionate and appropriately deleted afterwards.</p>

Data item	Short term event +1 month	Medium term individual at school +1 year	Long term individual at school +5 years	Very long term pupil is aged 25 or older	Justification
Medical information and administration	✓ (permission slips)	✓ (medical conditions and ongoing management)		✓ medical incidents (potentially)	To support any handover work about effective management of medical conditions to a subsequent institution. Permission forms that parents sign should be retained for the period that medication is given, and for 1 month afterwards if no issue is raised by child/parent. If no issue is raised in that time, that feels a reasonable window to assume all was administered satisfactorily. Adding this policy to the permission slip would seem prudent. Medical 'incidents' that have a behavioural or safeguarding angle (including the school's duty of care) should refer to the retention periods associated with those policies.
Health and safety information and administration			✓		Documentation regarding risk assessments and the testing or sampling of health and safety aspects will be retained for 5 years.
Safeguarding	✓				All data on the safeguarding file potentially forms part of an important story that may be needed retrospectively for many years. The elements of a pupil file (name, address) that are needed to identify children with certainty are needed to be retained along with those records. However, we shall pass all records to the child's new school when the pupil leaves us, keeping only a sheet that indicates the name of the child, their cohort and the date the file was handed over.

Data item	Short term event +1 month	Medium term individual at school +1 year	Long term individual at school +5 years	Very long term pupil is aged 25 or older	Justification
Special educational needs	✓				All data on the SEND file forms part of an important story that may be needed retrospectively for many years. However, we shall pass all records to the child's new school when the pupil leaves us, keeping only a sheet that indicates the name of the child, their cohort and the date the file was handed over.
Personal identifiers, contacts and personal characteristics	✓ (images used in identity systems)  ✓ (biometrics)	✓ (images used in displays in school)	✓ (postcodes)  ✓ (characteristics)		<p>Images are used for different reasons, and the reason should dictate the retention period. Images used purely for identification can be deleted when the child leaves the setting. Images used in displays etc. can be retained for educational purposes whilst the child is at the school. Other usages of images will be anonymised if the images record special events are displayed within the school.</p> <p>Biometric data should not be retained long after the activity that requested its use has finished (for example, the child no longer attends the school to have a meal).</p> <p>As set out in other sections, names are needed for smooth handover to subsequent schools for up to one year. Postcode data is useful in analysing longer-term performance trends or how catchment/pupil populations are shifting over time, but full address data (house number and road) is not required for that activity.</p> <p>Characteristics form an essential part of trend analysis, and so retention is in line with those needs.</p>
Staff Files		✓			These are archived once the staff member is no longer in employment, but destroyed after 5 years of their leaving.

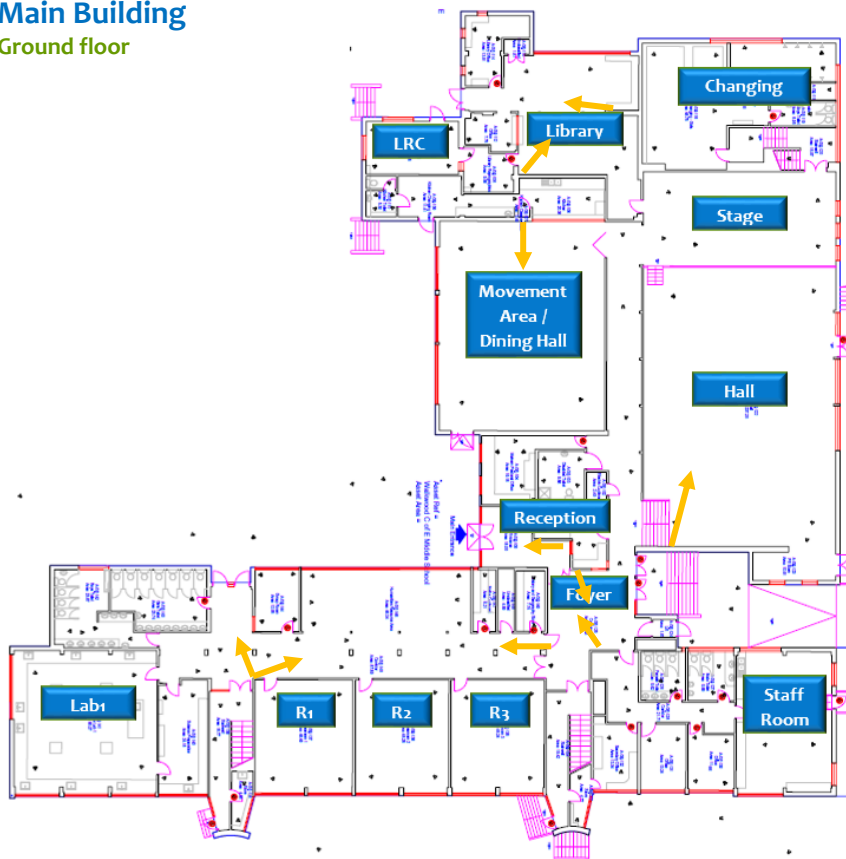
Data item	Short term event +1 month	Medium term individual at school +1 year	Long term individual at school +5 years	Very long term pupil is aged 25 or older	Justification
Recruitment	✓	✓			Any candidates' information is held for up to one year, it being destroyed at the end of the academic year in which the application was made. Successful applications information is held within their staff file. The equalities data is anonymised upon receipt, and the originals destroyed within 1 month of the recruitment interviews.
Governing Body minutes			✓		Documents will be stored for five years.





# Appendix 4: CCTV positions

## Main Building Ground floor

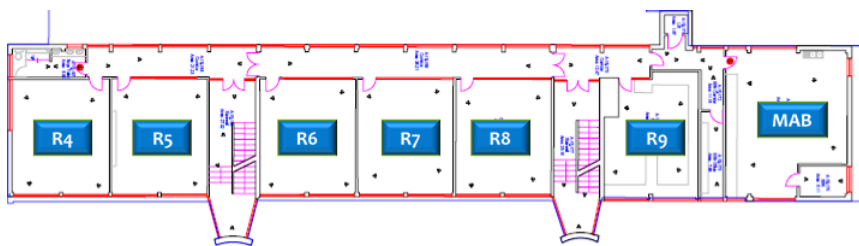


→ Internal cameras linked to digital recording

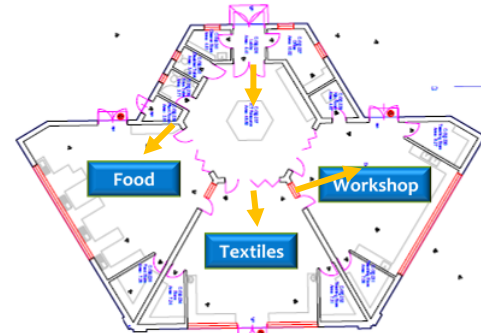
## Sub-ground floor



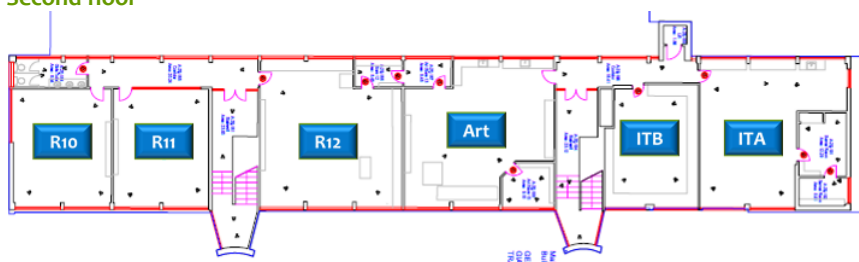
## First floor



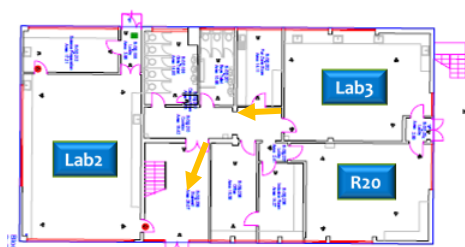
## Technology Building



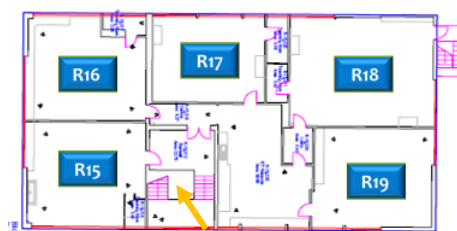
## Second floor

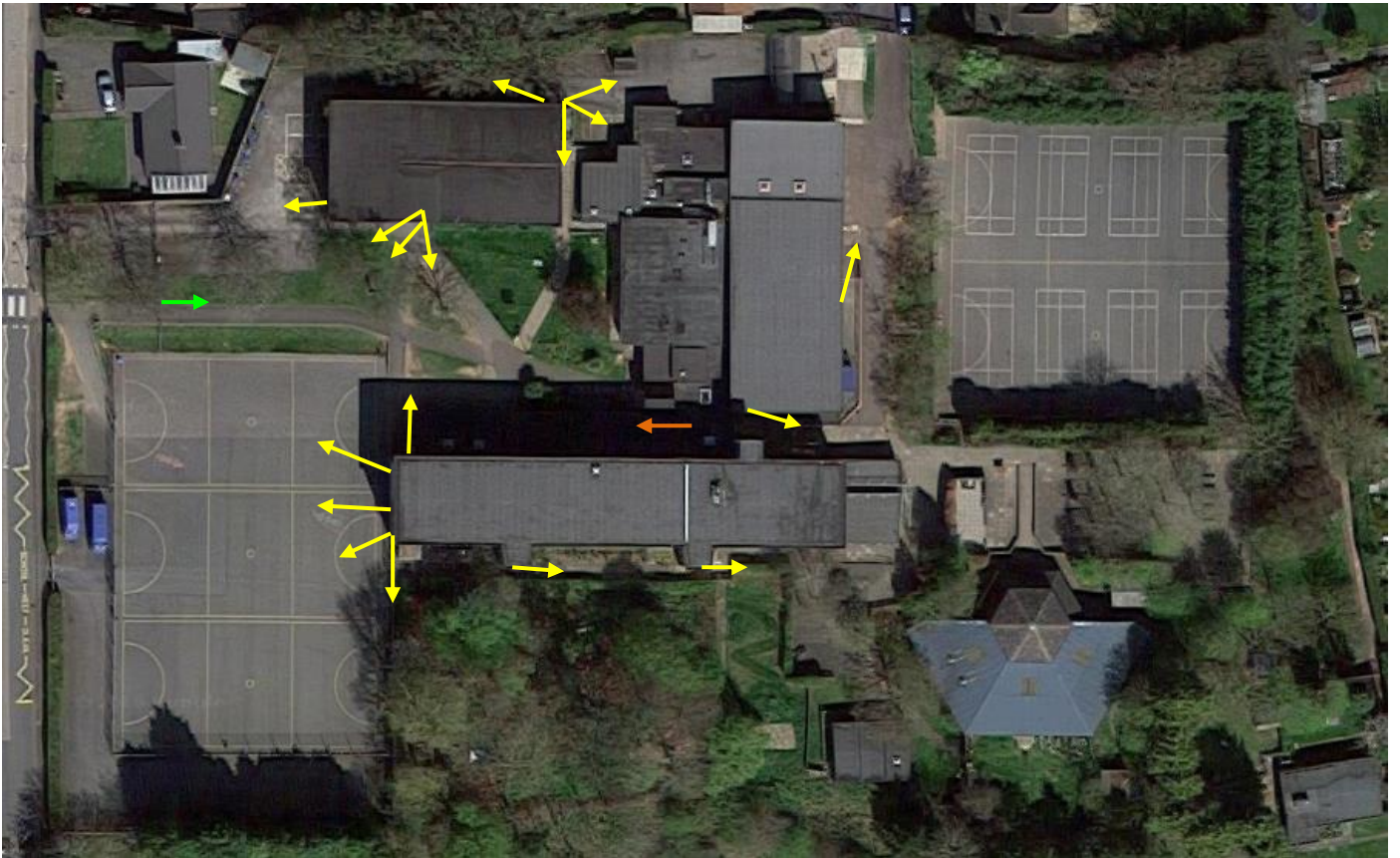





## Joy Vater Building Ground floor



## First floor





-  External cameras linked to digital recording
-  Internal camera with external view linked to digital recording
-  External cameras linked to monitor in Reception

