Woodlane High School

achieving success in a nurturing environment

Data Protection Policy

Updated: June 2025

Next Update: June 2027

Du Cane Road London W12 0TN
Tel: 0208 743 5668 | **Fax:** 0208 743 9138
Headteacher: Claire Maynard | **E-mail:** admin@woodlane.lbhf.sch.uk
Web: www.woodlane.lbhf.sch.uk

This document is a statement of the aims and principles of the School, for ensuring the confidentiality of sensitive information relating to staff, pupils, parents and governors.

Introduction

Woodlane High School needs to keep certain information about its employees, pupils, and other users to allow it to monitor performance, achievements, and health and safety. It is also necessary to process information so that staff can be recruited and paid, courses organised and legal obligations to funding bodies and government complied with. To comply with the law, information must be collected and used fairly, stored safely and not disclosed to any other person unlawfully.

1. Aims

Woodlane High 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 General Data Protection Regulation (GDPR) and the expected provisions of the *Data Protection Act 2018* (DPA 2018) as set out in the Data Protection Bill.

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

2. Legislation and Guidance

This policy does not form part of the contract of employment for staff, but it is a condition of employment that employees will abide by the rules and policies made by the School. Any failures to follow the policy can therefore result in disciplinary proceedings.

This policy meets the requirements of the GDPR and the expected 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 meets the requirements of the *Protection of Freedoms Act 2012* when referring to our use of biometric data.

It also reflects the ICO's code of practice for the use of surveillance cameras and personal information.

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

LGfL have provided a number of the templates required for school, including Subject Access Request responses and Breach Reports. Their model templates and other additional guidance can be found here: https://www.lgfl.net/gdpr

3. Definitions

3.1 The Data Controller

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

The school is registered as a data controller with the ICO and will renew this registration annually or as otherwise legally required.

3.2 Governing Body

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

3.3 Data Protection Officer

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

They will provide an annual report of their activities directly to the governing board and, where relevant, report to the board their advice and recommendations on school data protection issues.

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

Full details of the DPO's responsibilities are set out in their job description.

DPO for Woodlane High School is Tim Heapy and is contactable via 0208 743 5668 or dpo@woodlane.lbhf.sch.uk.

3.4 Headteacher

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

3.5 Additional Definitions

Personal data	Any information relating to an identified, or identifiable, individual. This may include the individual's: • Name (including initials) • Identification number • Location data • Online identifier, such as a username 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: • Racial or ethnic origin • Political opinions • Religious or philosophical beliefs • Trade union membership • Genetics • Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes • Health – physical or mental • 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. 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. Responsibilities of Staff

The term 'staff' may describe the school workforce under the following:

- Those who are directly employed by Woodlane High School (H&F) such as teachers and teaching assistants.
- Those indirectly employed through an agency, such as supply teachers, (e.g. Vibe), Apprentices, (e.g. Aspire ATA) or cleaners, (e.g. Purgo).
- Those employed by a company/organisation to work directly with the school, such as Speech and Language Therapists, (NHS) or staff delivering mental health therapy, (e.g. RESPOND).
- Those who support the school on a voluntary sense, such as the Governing Body or Friends of Woodlane.

4.1 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.
- Using approved methods and means of communication with others, such as using @woodlane email addresses rather than personal email accounts, and using school computers rather than personal devices.
- Contacting the DPO in the following circumstances:
    - With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
    - If they have any concerns that this policy is not being followed
    - If they are unsure whether 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

4.2 Responsibilities to Data Security

All staff are responsible for ensuring that:

- Any personal data that they hold or request is kept securely and personal data items are not kept on home computers, removable memory keys or cloud-based services that are not owned or operated by the school.
- If personal data is required, (i.e. Date of Birth/UPN to enter a pupil for a qualification), this is completed through a secure channel with a registered provider that the school has already vetted. Any paper copies are destroyed on completion of this task.

- Personal information is not disclosed either orally or in writing or via Web pages or by any other means, accidentally or otherwise, to any unauthorised third party

Staff should note that unauthorised disclosure will usually be a disciplinary matter, and may be considered gross misconduct in some cases. These responsibilities will be included within the school's handbook and code of conduct.

Personal information should:

- Be kept in a locked filing cabinet, drawer, or safe.
- If it is computerised, be coded, encrypted or password protected using school based hardware (or on the school's network drive) that is regularly backed up.
- If a copy is kept on a disk or other removable storage media, (i.e. School IPad or School Memory Keys) that media must itself be kept in a locked filing cabinet, drawer, or safe.

4.3 Responsibilities of Pupils

Pupils have a role to place in Data Security and are taught through their PSCHE and Computing lessons to be responsible with their private data, and that of their friends and family.

The overall responsibility for data protection does not fall on pupils however, (largely due to the nature of SEND), so staff and families are encouraged to fulfil this role more acutely in an SEND environment. Pupils who breach data responsibilities through their use of technology will be taught to better understand their actions.

5. Data protection principles

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

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

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

6. Collecting personal data

6.1 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 GDPR and Data Protection Act 2018.

If we offer online services to pupils, such as classroom apps, (i.e. Mathletics), and we intend to rely on consent as a basis for processing, we will get parental consent where the pupil is under 13 or we believe that the pupil's capacity to provide consent is impacted to a greater extent by their learning needs.

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

6.2 Limitation, minimisation and accuracy

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

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

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

When staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with the DFE's framework.
Woodlane has adopted the framework suggested by the DfE on Pages 54 to 62 of *Data Protection: A Toolkit for Schools*. An example of this guidance instructs us to remove data elements related to behaviour within one year of a pupil leaving Woodlane, whilst it details that schools should retain safeguarding information until a pupil reaches the age of 25. Please see the DfE guidance for further information.

7. Sharing personal data

7.1 Who do we share with?

We do not share information about our pupils, parents or staff without their being a legal bases for doing so, or without consent being provided. It is our policy to maintain a database of all

organisations we work with, our reasons for sharing information with them and the legal basis for this sharing, or that consent has been received.

7.2 Legal Obligation:

We are required to share information about our pupils and staff with our local authority and the DfE under section 3 of The Education Regulations 2013. This data sharing underpins school funding and educational attainment policy and monitoring. The sharing of this data is covered by our *legal obligation*, these organisations include:

- Hammersmith & Fulham (or your own local authority).
- The Department for Education (DfE).
- Disclosure and Barring Service (DBS).
- The Woodlane High School Governing Body.

7.3 Public Task:

The school shares data with other providers as a *public task*, which allows us to undertake actions to in order for the school to run properly. This enables us to fulfil our duty to each young person to ensure pupils' needs are being fully met and the correct services are being provided. For staff it may enable them to be paid, or ensure safeguarding procedures are met. Different types of data will be shared depending on the type of roll these organisations have. These organisations/groups include:

- Speech & Language Therapists (through NHS CLCH if required within an EHCP).
- Occupational Therapists or Physiotherapists (through CLCH if required within an EHCP).
- Mental Health provision within the school, operated by RESPOND, Anna Freud Centre and MIND.
- Virtual Schools (for Looked After Children).
- Examining Bodies (i.e. AQA, Edexcel, OCR, WJEC, NCFE, etc.)
- Our Regulator (i.e. Ofsted)
- The School Nurse (for specific areas of need).
- The pupil's family and representatives.
- Youth support services through the local authority or commissioned services for pupils aged 13 and over.
- A school/college/sixth form that the pupil is applying to, or is expecting to attend after leaving Woodlane.
- SIMS, (or a similar Management Information System as determined by the school).
- Turniton who manage the school's computer network.
- LGfL who manage the school's network filter.
- GL Assessment who host online CAT and PASS tests for pupils and require names, ages, etc. to ensure feedback is appropriate to their individual circumstances.
- Prospects who are the school's payroll provider.
- BSquared who provide the assessment system that the school uses to track progress.
- Mitie, (changing to The Pantry September 2023) who provide school lunches on site and require allergy/medical information.
- Evolve who are the school's online risk assessment service for educational visits.

- Governor Hub which provides a platform for the school's Governors to meet, share information and store school information securely. Only accessible by school Governors, (DBS checked) and agreed partners, e.g. Clerk.
- Trade unions and associations that support staff in their role.
- Health and social welfare organisations/authorities that support staff in their role.
- Security organisations, including those managing school security systems, (i.e. Chubb), or those working in the wider community (i.e. Prevent).
- Professional bodies, advisers and consultants that support staff in their role.
- Charities and voluntary organisations.
- Police forces, courts, tribunals, where this is requested by these organisations.

7.4 Vital Task:

In an emergency, the school will engage with other providers through our *vital interest*, which allows us to undertake actions to protect someone's life. The most likely scenario would be sharing pupil or staff information with a paramedic if they are admitted to hospital or sharing personal data to The Metropolitan Police in an emergency.

7.5 Legitimate Interest:

The school will, from time to time, engage with services that will support the education of a pupil. Although these areas could reasonably be assumed to be a *legitimate interest*, there are occasions where a pupil's personal information (name/date of birth) may be required for registration or to set up an account. Parents and pupils have a choice as to whether their data is shared with these organisations. **The following list is not exhaustive and should be read for reference only. Parents will be contacted for specific consent when necessary and their responses recorded.**

These organisations include:

- Mathletics
- Accelerated Reader
- London Youth Games
- SEN Swim
- Optional NHS Services (i.e. vaccinations and dental inspections)
- QPR Community Sports Team
- Bikeworks
- TFL
- Careers Hub

8. Rights of individuals

8.1 The right to be informed

Under the General Data Protection Regulations (GDPR), organisations are required to ensure that provision of individual rights are made and this policy reflects these rights.

The 'right to be informed' encompasses the school's obligation to provide 'fair processing information'. We meet our obligation by issuing Privacy Notices to staff and parents which are published online. Information supplied by Woodlane High School is:

- Concise, transparent, intelligible and easily accessible. The Privacy Notice adopted by Woodlane High School is concise, and outlines the purpose of data collection along with details of third parties with whom we may share that information. It is issued to staff on appointment and annually thereafter. An electronic version is stored on the school network.
- Written in clear, plain English
- Free of charge

8.2.1 The Right of Access (Subject Access Requests)

Woodlane High School Staff, and parents of children attending the school have the right to obtain:

- 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.

The GDPR clarifies that the reason for allowing individuals to access their personal data is so that they are aware of, and can verify the lawfulness of, the processing. Requests for access are referred to as *Subject Access Requests*.

Subject access requests must be submitted in writing, either by letter, email or fax to the DPO. They should include:

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

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

8.2.2 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 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 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. This is particularly significant given the varying degrees of understanding due to pupil's SEND at Woodlane High School.

8.2.3 Responding to Subject Access Requests

Subject Access Requests are handled by the DPO, acting for the school as data controller.

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 if it is repetitive, or asks for further copies of the same information.

When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO.

8.2.4 Issuing Information

Information may be supplied electronically or in paper format. An analysis will be made to determine which of the formats is the most appropriate and the decision will be agreed between the person making the request and the school. In the event that the information is supplied electronically it will be provided in PDF format.

Whilst the GDPR recommends good practice for the individual making the request to be access a self-service portal, this is not possible at Woodlane High School.

8.3.1 The Right to Rectification (Accuracy)

The GDPR gives individuals the right to have personal data rectified if it is inaccurate or incomplete.

8.3.2 Rectification Timeframe

Woodlane High School will respond to individuals within one month. Where the request for rectification is complex, the school reserves the right to extend this timeline to two months.

In the event that the school is not taking action in response to a request for rectification we will explain to the individual, in writing, and outline the reasons for this along with their right to complain.

8.3.3 Right to rectification – Third Parties

Where a third party has information about an individual that requires rectification, the school will inform those parties without undue delay.

8.4.1 The Right to Erasure

The right to erasure is also known as the 'right to be forgotten'. The broad principle underpinning this right is to enable an individual to request the deletion or removal of personal data where there is no compelling reason for its continued processing.

8.4.2 When This Applies

Individuals have the right to have personal data erased and to prevent further processing in specific circumstances:

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed.
- When the individual withdraws consent.
- When the individual objects to the processing and there is no overriding legitimate reason for continuing the processing.
- The personal data was unlawfully processed (ie in breach of GDPR).
- The personal data has to be erased in order to comply with a legal obligation.
- The personal data is processed in relation to information society services to a child.

Under the GDPR, the right to erasure is not limited to processing that causes unwarranted and substantial damage or distress. However, if the processing does cause unwarranted and substantial damage or distress the case for erasure will be strengthened.

8.4.3 Refusal to Comply

In accordance with data protection legislation, Woodlane High School has the right to refuse to comply with requests for erasure where the personal data is processed for the following reasons:

- To exercise the right of freedom of expression and information.
- To comply with a legal obligation for the performance of a public interest task or exercise of official authority.
- For public health purposes in the public interest.
- Archiving purposes in the public interest, scientific research, historical research or statistical purposes.
- The exercise or defence of legal claims.

8.4.4 The Right to Erasure of Children's Data

Schools have the right to collect pupil data in order to carry out its legal obligation for the performance of a public interest task. However, the GDPR enhances protection of children's data particularly in relation to online environments. Where consent has been given and a request for erasure is later received the school will remain mindful that the initial consent may have been given without full awareness of the impact of its use.

8.4.5 Informing Third Parties of Erasure

Where the school has disclosed personal data to third parties Woodlane High School will inform those parties, without undue delay, about the personal data erasure unless it is impossible or involves disproportionate effort to do so.

Woodlane High School does not share personal data in any online environment without explicit consent.

8.5.1 The Right to Restrict Processing

Individuals have the right to block or supress processing of personal data. In these instances, Woodlane High School shall be permitted to store data but not to process it further.

8.5.2 Applying the Right to Restrict Processing

The school shall be required to restrict processing in the following circumstances:

- Where an individual contests the accuracy of the personal data the school will restrict further processing until the accuracy of the personal data has been verified.
- Where an individual has objected to the processing (where it was necessary for the performance of a public interest task or purpose of legitimate interests), and the school is considering whether its legitimate reasons override those of the individual.
- When processing is unlawful and the individual opposes erasure and requests restriction instead.
- If the school no longer needs the data but the individual requires it to establish, exercise or defend a legal claim.

8.5.3 Informing third parties of restriction of processing

Where personal data becomes subject to restriction of processing and has been disclosed to a third party, Woodlane High will inform the third party, without undue delay, unless it is impossible or involves disproportionate effort to do so.

When the school decides to lift a restriction on processing it must inform the individual.

8.6.1 The Right to Object

Individuals have the right to object to:

- Processing based on legitimate reasons or the performance of a task in the public interest/exercise of official authority
- Direct marketing
- Processing for purposes of scientific/historical research and statistics

8.6.2 Compliance with the Right to Object for the Performance of a Legal Task

Individuals must have an objection on ‘grounds relating to his or her particular situation’. Woodlane High School will stop the processing of personal data unless:

- We can demonstrate compelling legitimate grounds for the processing, which overrides the interests, rights and freedoms of the individual.
- The processing is for the establishment, exercise or defence of legal claims.

Individuals are informed of their right to object within the school's privacy notices. We will also inform individuals of their right to object at the point of the first communication and will be 'explicit and presented clearly'.

8.7 Parental Request 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.

8.9 Other Rights of the Individual

In addition to the rights above individuals also have the right to:

- 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 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.

9. Biometric Recognition Systems, CCTV & Photography

9.1 Biometric Entry

Where we use pupils' biometric data as part of an automated biometric recognition system (for example, pupils and staff can use finger prints to access the site, we comply with the requirements of the Protection of Freedoms Act 2012.

Parents/carers have been notified before the biometric recognition system was put in place and before their child first takes part in it. The school has received written consent from at least one parent or carer before taking 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. We continue to provide alternative means of accessing the school site for those pupils.

Parents/carers and pupils can object to participation in the school's biometric recognition system, 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 parents/carers.

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

9.2 CCTV

We use CCTV in various locations 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 the DPO.

9.3 Photography & Video

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

We have reviewed our consent forms, and now ask for written consent from parents/carers in three areas:

- Taking photos and videos and using them internal for displays/pupil books.
- Taking photos and videos for use on the school website.
- Taking photos and videos for use in external marketing, i.e. school prospectus.

When asking for consent, we will clearly explain to both the parent/carer and pupil how the photograph and/or video will be used.

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.

10. Data Protection by Design

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.
- 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 (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
- Maintaining records of our processing activities, including:
    - For the benefit of data subjects, making available the name and contact details of our school 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, 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 (specified in Woodlane High School – Legal Basis and Retention Audit)

11. Data Security and Storage of Records

11.1 Security and Storage

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. Staff are expected to only use Woodlane approved external memory devices.
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices.
- 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 demonstrate the need to have access to this data, how it will be processed, and confirm it is returned or destroyed after the activity takes place.
- Where a data processor that the school works with requires personal data, the school will ensure checks on compliance are carried out. This is essential if the organisation use overseas servers, which may not be bound by the same regulations.
- Passwords that are at least 8 characters long containing letters and numbers are used to access school computers, laptops and other electronic devices. Staff and pupils are reminded to change their passwords at regular intervals.
- Staff, pupils or governors must not store personal information on their personal devices. The only exception is school emails linked to mobile phones for members of the SMT who may require access to these in an emergency, or to ensure the efficient operation of the school. In these circumstances, the SMT are expected to follow the same security procedures as for school-owned equipment, including using both passwords and biometrics to ensure the upmost security. Staff will delete any personal data (i.e. in a downloaded pdf) immediately.

- 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.

11.2 Disposal of Records and Retention

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 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.

When disposing of/destroying files, we will complete the school's *List of School Records and Data Safely Destroyed* log to keep track of this. Appendix 3

11.3 Retention Policy

The school have adopted the majority of recommended retention policies drafted by the DfE and published by LgFL/3BM. The retention policy is stored within the Woodlane High School – Legal Basis and Retention Audit, shared with the Governing Body prior to the implementation of GDPR and reviewed within one year. The recommendations were scrutinised by the DPO and the School's Business Manager.

In some instances, these recommendations were adapted to meet the specific requirements of Woodlane High School. Unique to a special educational needs environment, all pupils on roll have SEND, therefore retention of their basic data (recommended: age of 25) has to be extended to other aspects of the pupil record, e.g. exclusions. Some aspects, such as whether the pupil was eligible for free school meals (FSM) are only required for as long as this could be useful for financial matters (6 years) which follows recommended guidelines.

The retention policy document contains colour coding which denotes where recommendations have been adopted (green), where they have been adapted due to the specific needs of the school, and there is a legal basis for doing so (red).

Retention of Governing Body minutes and documents have their own specific retention policy, which is part of an annual audit. Copies of all minutes and documents are maintained by the School's Business Manager and the Clerk to the Governing Body. Many documents are a matter for public record, and as such have to be maintained in a state that can be shared at request. Governor documents that contain sensitive content (confidential) are retained for 10 years following a meeting, whereas the standard published meeting documents are retained for 6 years.

LGfL control and process many elements of school data on behalf of the school, including email, MIS data and passwords (USO). Therefore, the school must ensure that LGfL's policy on retention matches our own. This is available here: LGfL Policy – Retention and Disposal. The school ensures that this is reviewed alongside our own policy.

11.4 Disciplinary, Grievance and Exceptions

Where disciplinary procedures are taken against a member of staff, these become part of the personal file, e.g. a written warning for conduct, capability proceedings, etc. To ensure compliance

with the legal framework, advice was sought from YESS and Headsup. The personal file is retained for 6 years following termination of employment.

This process is also relevant where a grievance has been submitted by a member of staff, or the grievance is specifically related to a member of staff. This is also retained for 6 years following termination of employment.

Exceptions to the above would be in cases that relate to allegations of child protection matters and safeguarding, which would be retained until the pupil is at least 25 years old, or indefinitely depending on the case. These exceptions apply as there may be a legal requirement to investigate historic cases.

11.5 Automated Removal

Some specific data points, such as the school's CCTV camera footage (approximately 1 month) and the daily cloud backup of the school's computer storage systems (3-day record/re-write cycle) are automated and re-written as per the cycle.

The school aims to bring more records, including certain data contained within the School Information Management System (SIMS) in to a cycle of automated removal. This process is on-going as SIMS adapt systems to make this possible.

12. Personal Data Breaches

The school will make all reasonable endeavours to ensure that there are no personal data breaches. In the unlikely event of a suspected data breach, we will follow the procedure set out in Appendix 1. When appropriate, we will report the data breach to the ICO within 72 hours. Such breaches in a school context may include, but are not limited to:

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

The school will record all data breaches in the Data Breach Record (Appendix 2).

13. Training

All staff and governors are provided with data protection training as part of their induction process. Current staff continue to receive information in the form of this policy, a code of conduct and twilight at the start of each academic year.

Data protection forms part of continuing professional development, where changes to legislation, guidance or the school's processes make it necessary.

The DPO attends training regularly to remain up to date with current regulations and best practice.

14. Monitoring Arrangements

The DPO 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.

15. Cyber Security

The school has adopted the LGfL policy for Cyber Security. There are some necessary crossovers with other parts of this policy, however all parts of the policy and systems should work together to protect the school's data, and that of the staff, pupils, parents and partners.

A cybersecurity incident can have a major impact on any organisation for extended periods of time. For a school, this can range from minor reputational damage and the cost of restoring systems from existing backups to major incidents such as losing student work or access to learning platforms and safeguarding systems, which could lead to data-protection fines or even failing an inspection.
This Cybersecurity Policy outlines Woodlane High School's guidelines and security provisions which are there to protect our systems, services and data in the event of a cyberattack.

This part of the school's data policy applies to all Woodlane High School staff, contractors, volunteers and anyone else granted permanent or temporary access to our systems and hardware. It also covers the physical and technical elements that are used to deliver IT services for the school.

15.1 Cyber Security Risk Management

Woodlane High School include cybersecurity risks and potential data protection breaches via the Data Breach Record, (appendix 2 of the Data Policy) regularly reporting on the progress and management of these risks to Governors 3 times a year.

15.2 Physical Security

Woodlane High School ensure there is appropriate physical security and environmental controls protecting access to its IT Systems, including but not limited to air conditioning, lockable cabinets, and secure server/communications rooms.

15.3 Asset Management

To ensure that security controls to protect the data and systems are applied effectively Woodlane High School will maintain asset registers (defined as the school's Inventory) for, files/systems that hold confidential data, and all physical devices (servers, switches, desktops, laptops etc) that make up its IT services.

15.4 User Accounts

Users are responsible for the security of their own accounts. If at any time they believe their credentials may have been compromised, for example after a phishing scam, they must change their password and inform Turniton as soon as possible. Personal accounts should not be used for work purposes. Woodlane High School will implement multi-factor authentication where it is practicable to do so, particularly for those assets with the highest level of risk associated.

15.5 Devices

To ensure the security of all Woodlane High School issued devices and data, users are required to:

- Lock devices that are left unattended
- Update devices when prompted
- Report lost or stolen equipment as soon as possible to the Data Protection Officer, (DPO) and Turniton
- Change all account passwords at once when a device is lost or stolen (and report immediately to the DPO and Turniton
- Report a suspected threat or security weakness in Woodlane High School 's systems to DPO

Devices will be configured with the following security controls as a minimum:

- Password protection
- Full disk encryption
- Client firewalls
- Anti-virus / malware software (automatically this is Sophos if it is a school managed device
- Automatic security updates
- Removal of unrequired and unsupported software
- Autorun disabled
- Minimal administrative accounts

15.6 Data Security

Woodlane High School will take appropriate measures to reduce the likelihood of the loss of availability to, or the disclosure of, confidential data.

Woodlane High School's defines confidential data as:

- Personally identifiable information as defined by the ICO
- Special Category personal data as defined by the ICO
- Unpublished financial information

Critical data and systems will be backed up on a regular basis following the 3-2-1 backup methodology

- 3 versions of data
- 2 different types of media
- 1 copy offsite/offline

Woodlane High School uses Gridstore, (provided by LGfL) as an online backup for all school data. This is operating effectively, and any school receive urgent communication if an element of this backup fails. See gridstore.lgfl.net

15.7 Sharing Files

Woodlane High School recognises the security risks associated with sending and receiving confidential data. To minimise the chances of a date breach users are required to:

- Consider if an email could be a phishing email or that a colleague's account could be 'hacked'. If something does not feel right check with the sender by another method, particularly in relation to financial transactions, attachments, or links to websites. School

staff, (in particularly those with financial responsibilities) have had regular training and increased awareness of these dangers
- Wherever possible, keeping Woodlane High School's files on school systems
- Not sending school files to personal accounts
- Verifying the recipient of data prior to sending
- Using file encryption where possible, sending passwords/keys via alternative communication channels
- Alerting [IT Support/DPO] to any breaches, malicious activity or suspected scams

15.8 Training

Woodlane High School recognises that it is not possible to maintain a high level of Cybersecurity without appropriate staff training. The school integrates regular Cybersecurity training into Inset days, provides more specialist training to staff responsible for maintaining IT systems and promotes a "No Blame" culture towards individuals who may fall victim to sophisticated scams.

15.9 System Security

Turniton and LGfL build security principles into the design of IT services for Woodlane High School

- Security patching – network hardware, operating systems and software
- Pro-actively plan for the replacement of network hardware, operating systems and software before vendors stop providing security support for them
- Actively manage anti-virus systems
- Actively manage and test backups
- Regularly review and update security controls that are available with existing systems
- Segregate wireless networks used for visitors' & staff personal devices from school systems
- Review the security risk of new systems or projects
- Provide weekly reports in to filtering and monitoring process, including commonly refused websites

15.10 Responding to a Major Incident

Woodlane High School will develop, maintain, and regularly test a Cybersecurity Major Incident Response Plan. The school will not publish this outwardly. The plan will include identifying or carrying out:

- Key decision-makers
- Key system impact assessments and restoration priorities (i.e. which backups needs to be restored first for the school to become operational again)
- Emergency plans for the school to function without access to systems or data
- Alternative methods of communication, including copies of contact details
- Emergency budgets and who can access them / how
- Key agencies for support (e.g. IT support company)

15.11 Maintaining Security

Woodlane High School understands that the financial cost of recovering from a Major Cybersecurity Incident can far outweigh the ongoing investment in maintaining secure IT systems Woodlane High School will budget appropriately to keep cyber related risk to a minimum.

18. Use of Artificial Intelligence (AI)

Artificial Intelligence (AI) refers to computer systems that can perform tasks typically requiring human intelligence, such as processing natural language, generating content, making predictions, and analysing data. Examples include tools like ChatGPT, image generators, and AI-powered functions in platforms such as Microsoft Office, Canva, and Arbor.

This element of the school's data policy is designed to promote the safe, ethical, and responsible use of AI tools by students, staff, and members of the school community. It aims to ensure AI is used to enhance teaching and learning, while safeguarding against potential misuse. It also supports the development of digital literacy, critical thinking, and awareness of the limitations and risks associated with AI.

The policy complements other key school documents, including the Safeguarding, E-Safety, Acceptable Use, Examinations, and Teaching & Learning policies. It applies to all use of AI technologies on school premises or remotely, whether on school-owned or personal devices. All AI use within the school is subject to regular monitoring to ensure alignment with educational goals, safeguarding principles, and data protection regulations.

The school uses AI responsibly within various educational and administrative applications, including:

- **Arbor** – for pupil information management, data analysis, and summarising key pupil information for external agencies.
- **Canva** – for designing and creating teaching and learning resources.
- **Office 365** – for content generation, document summarisation, and productivity enhancements including drafting pupil reports.
- **Twinkl** – for supporting lesson planning and generating classroom materials.
- **Other applications** – for creating engaging and accessible teaching and learning resources

18.1 Legitimate Use

AI tools may be used in the classroom with teacher supervision, provided they are age-appropriate and align with curriculum aims. Pupils receive guidance on the advantages and risks of AI use through lessons exploring its role in education, business, and wider society.

All AI tools used must be school-approved and comply with data protection and safeguarding requirements. Staff are responsible for reviewing AI-generated content and remain accountable for all materials used or shared.

18.2 Areas of concern

While AI can support learning and productivity, its misuse presents challenges and potential risks. For concerns specific to coursework or examinations, please refer to the school's Examination Policy.

Key areas of concern include:

- **Academic integrity:**
    - Pupils must not use AI to cheat, plagiarise, or produce content dishonestly.
    - Any AI-assisted work must be clearly acknowledged and authorised by teaching staff.
- **Responsible use:**
    - Pupils and staff must avoid excessive dependence on AI tools.
    - Emphasis should remain on critical thinking, independent learning, and creativity.
- **Data protection and privacy:**
    - Uploading personal, sensitive, or identifiable data into AI tools is strictly prohibited.
    - Images of pupils or staff must not be used with AI applications unless explicitly approved for school-authorised projects.

All AI tools used must meet GDPR compliance standards and uphold the privacy of staff and students. Misuse of AI may be treated as a violation of the Acceptable Use or Behaviour Policy. Any breaches or concerns should be reported to the e-safety Lead or the Designated Safeguarding Lead (DSL).

For questions or concerns related to AI, please contact the e-safety Lead or DSL.

Personal data breach procedure

Appendix 1

This procedure is based on guidance on personal data breaches produced by the ICO.

- On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the DPO
- The DPO will investigate the report, and determine whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidentally or unlawfully:
    - Lost
    - Stolen
    - Destroyed
    - Altered
    - Disclosed or made available where it should not have been
    - Made available to unauthorised people
- The DPO will alert the Headteacher and the chair of governors
- The DPO will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary. (Actions relevant to specific data types are set out at the end of this procedure)
- The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen
- The DPO will work out whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the DPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:
    - Loss of control over their data
    - Discrimination
    - Identify theft or fraud
    - Financial loss
    - Unauthorised reversal of 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 DPO must notify the ICO.
- The DPO will document the decision (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored in a Data Breach Record on the school server.

- Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website within 72 hours. https://ico.org.uk/for-organisations/report-a-breach/personal-data-breach/
- As required, the DPO will set out:
    - A description of the nature of the personal data breach including, where possible:
        - The categories and approximate number of individuals concerned
        - The categories and approximate number of personal data records concerned
    - The name and contact details of the DPO
    - A description of the likely consequences of the personal data breach
    - A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned
- If all the above details are not yet known, the DPO will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible
- The DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPO will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:
    - The name and contact details of the DPO
    - A description of the likely consequences of the personal data breach
    - A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned
- The DPO will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies
- The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:
    - Facts 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 in the Data Breach Record form in a secure area of the school server.
- The DPO and Headteacher will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible

Actions to minimise the impact of data breaches

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

Data Breach Record

Appendix 2

A Data Breach Record must be completed by the DPO or the most suitable person to report the breach. This should be completed following any reports of a security breach or potential breach involving personal data. Staff must follow the school's *Personal Data Breach Procedure* identified in Appendix 1 of the Data Policy 2018 following notification of a breach or potential breach. The school must ascertain whether the ICO should be informed about notifiable breaches within 72 hours.

Information	Response
Date and time this record completed	
Name of person completing this record	
General description of the breach	
Name of person who made the report of the breach / potential breach	
Date and time the breach / potential breach was reported	
Who was the breach / potential breach reported to?	
Has the Data Protection Officer been informed?	**Y | N**
Has the Personal Data Breach Procedure been followed?	Y | N
What are the details of the breach / potential breach (include as much detail as possible) NB: A separate investigation must be undertaken where appropriate	

Information	Response
Who is responsible for the breach i.e. the school as data controller, a joint data controller or a data processor?	
Is the breach ongoing or has it been contained?	
Is any other information required in order to assess the extent of the breach / the risk to data subjects? If so, specify that information here.	
Whose data has / may have been compromised as a result of the breach / potential breach?	
Type of data involved	
Does the breach / potential breach involve sensitive personal data or information about criminal offences?	**Y | N**
What is the risk to individuals?	
Is there likely to be a high risk to individuals?	**Y | N**
Does the breach need to be reported to the ICO? If yes, and if the breach happened more than 72 hours ago, what is the reason for the delay if notifying the ICO	**Y | N**
If the breach has already been reported to the ICO, give date and time report was made and who made the report	
If a report to the ICO is not being made, confirm the reasons why. Does that decision needs to be kept under review?	
Do the data subjects affected need to be notified about the breach? If so, confirm who will notify them and how and when they will be notified.	

Information	Response
If data subjects are not going to be informed, explain the reasons why.	
Does the breach need to be reported to the Police?	**Y | N**
Is there likely to be press / media interest as a result of the breach? **If so, have the appropriate protocols for handling media enquires been followed?**	**Y | N**
Outline the actions that need to be taken in response to the breach / potential breach to reduce the risk of a re-occurrence and who is responsible for implementing them and the relevant timescales. This should include whether an investigation under the school's disciplinary policy is recommended.	
Do any other steps need to be taken? e.g. comms to stakeholders, provision of complaints policy, consult legal advisors, notify insurers, external IT support.	

List of School Records and Data safely destroyed **Appendix 3**

The following sheet can be completed or alternatively documented in a spreadsheet when destruction of data/records takes place.

Date of destruction:

Staff member responsible:

Destroyed by:

Ref Number	File/Record Title	Description	Reference or Cataloguing Information	Number of Files Destroyed	Method of destruction	Confirm (i) Safely destroyed (ii) In accordance with Data Retention Guidelines Tick (√)
e.g.	*School Invoices*	*Copies of purchase invoices dated 2011/12*	*Folders marked "Purchase Invoices 2011/12" 1 to 3*	*3 Folders*	*Shredding*	√
1						
2						
3						
4						
5						
6						
7						
8						
9						
10						

School Information and Assets Audit and Log

Appendix 4

NB: This file is stored as a spreadsheet within the GDPR Folder.

Senior Information Risk Owner (SIRO): Claire Maynard **Last updated:** 10/06/2025

Data Protection Officer (DPO): Tim Heapy **By:** TH

Data Controller: Various

Data Processor: Various

Data held or collected by the school	Data label *	Information Asset Owner	Who has role / access to enter information	Where is the data kept?	Purpose	Legal basis for collection A* (IMPORTANT - you must be aware of this basis)	If Consent selected in previous column, when is it sought?	If Consent, where is record of consent stored?	How long is data item kept / used for?*
Pupil data (within MIS)									
Pupil records	Special Categories of Personal Data*	Headteacher	SAO/office administrators	EHCP Drive on Network, SIMS and hardcopy in SLT Office	Teaching and Learning /statutory returns	Legal obligation			Until child is 25 years old
Safeguarding / Child Protection data	Special Categories of Personal Data*	Headteacher	Head / named child protection officer	Safeguarding Folder on Secure Network area, CPOMS and hardcopy in Headteacher Office	Teaching and Learning /statutory returns	Protect vital interests			Indefinitely
SEN	Special Categories of Personal Data*	Headteacher	SENCO/SAO / class teachers / Deputy	EHCP Drive on Network, SIMS and hardcopy in SLT Office	Teaching and Learning /statutory returns	Legal obligation			DOB + 25 years
EAL	Special Categories of Personal Data*	Headteacher	EAL Lead / administrator	SIMS and hardcopy in SLT Office	Teaching and Learning /statutory returns	Legal obligation			part of pupil record
Exclusion, behaviour	Special Categories of Personal Data*	Headteacher	Class teacher / Pastoral tutor / Headteacher	Behaviour folder on Secure Network area, CPOMS and hardcopy in Headteacher Office	Teaching and Learning /statutory returns	Legal obligation			part of pupil record

Reports	Special Categories of Personal Data*	Headteacher	Class teacher / Pastoral tutor / Headteacher	Assessment and Reporting Folder on School Network	Teaching and Learning /statutory returns	Public interest/official authority			part of pupil record
Examination results / Statutory Assessments	Personal* Data	Headteacher/Exams Officer	Teachers / Exams Officer/Head of Dept.	Encrypted, password protected USB drive	Teaching and Learning /statutory returns	Public interest/official authority			part of pupil record
Attendance registers	Personal* Data	Headteacher	Class teachers / office administrators	SIMS	Safeguarding / Child Protection	Public interest/official authority			Date of entry + 3 years
Student photos	Special Categories of Personal Data*	Various	SAO/office administrators / class teachers	School Network	Safeguarding / Child Protection	Explicit consent	When student joins roll.	New School Starter Booklet filled in and stored as hard copy. SIMS updated with details.	retained on pupil record
Staff data (within MIS)									
Staff Personal File	Special Categories of Personal Data*	SBM	SAO/office administrators	SIMS and hardcopy in Headteacher office	Teaching and learning /statutory returns	Legal obligation			Termination of employment + 6 years
Performance / CPD data	Personal* Data	Headteacher	SAO/Bursar / Deputy	Performance Management Folder on Secure Network area	Teaching and learning /statutory returns	Public interest/official authority			part of personal file
Staff absence data	Special Categories of Personal Data*	Headteacher	SAO/ Deputy	MIS	Business Continuity / communication	Legal obligation			part of personal file
Staff photos	Special Categories of Personal Data*	Various	SAO/office administrators	Website, InVentory and School Photos folder	Business Continuity / communication	Explicit consent	When photos are taken.	Staff offered choice of photos. Consent	part of personal file
Other Personnel Data									
Recruitment records for new headteacher	Special Categories of Personal Data*	Governing Body	SAO / Recruitment Panel	Recruitment folder and Governor Hub	Business Continuity / communication	Legal obligation			Date of recruitment + 6 years

Recruitment of new staff	Special Categories of Personal Data*	Headteacher	SAO / Recruitment Panel	Paper copies printed and stored as required in Headteacher's office, emailed copies stored within outlook and backups in Funding Agreement folder.	Business Continuity / communication	Legal obligation			Successful = part of personal file. Unsuccessful = within 6 months.
DBS / vetting checks	Special Categories of Personal Data*	Headteacher	Head / SAO	Log details in SCR, (CPOMS/Staffsafe now used) and DBS Update Service. Login details stored within SIMS with limited access and deleted when left. DBS number moved to an archive after leaving.	Business Continuity / communication	Legal obligation			part of personal file
Appraisal / CPD data	Special Categories of Personal Data*	Headteacher	SAO/Bursar / Deputy	Performance Management Folder on Secure Network area	Teaching and learning /statutory returns	Public interest/official authority			part of personal file
Disciplinary and grievance records	Special Categories of Personal Data*	Headteacher	Head / SLT / Panel	SMT Drive and Hardcopies in Staff File in Headteacher Office	Safeguarding / Security	Public interest/official authority			part of personal file
Allegation of a child protection matter	Special Categories of Personal Data*	Headteacher	Head / Panel	CPOMS and Staff File	Safeguarding / Child Protection	Legal obligation			Indefinitely
Malicious allegation of a child protection matter	Special Categories of Personal Data*	Headteacher	Head / Panel	CPOMS and Staff File	Safeguarding / Child Protection	Legal obligation			Seek advice on a case by case basis
Health and safety assessments	Public data	SBM	H&S lead / teachers	Paper copies printed, emailed copies stored within HR drive with limited access.	Safeguarding / Security	Public interest/official authority			Date of meeting + minimum 3 years, then review
Health and safety accident reports	Special Categories of Personal Data*	SBM	H&S lead / Head / site manager	CPOMS and Staff File	Safeguarding / Security	Public interest/official authority			For each event, take advice as depends on nature of event
Admissions papers (successful or unsuccessful)	Personal* Data	Headteacher	Head / SLT	Paper copies printed and stored as required in Headteacher's office, emailed copies stored	Teaching and Learning /statutory returns	Legal obligation			Successful = part of pupil record. Unsuccessful = case resolution + 1 year

				within outlook and backups in Funding Agreement folder.					
Student medical records and reports	Special Categories of Personal Data**	Headteacher	Nurse / SLT / class teacher	EHCP Drive, Evolve and in Pupil Files.	Safeguarding / Child Protection	Legal obligation			DOB + 25 years
Student social service records and reports	Special Categories of Personal Data**	Headteacher	SS staff / SLT / class teacher	CPOMS, Pupil Files and EHCP Drive.	Safeguarding / Child Protection	Legal obligation			DOB + 25 years
Student file - mid-year transfer to public school with no requirement to share.	Special Categories of Personal Data**	Headteacher	Offered to new school	Hard copies of file. SIMS CTF.	Teaching and Learning /statutory returns	Public interest/official authority			File will be sent to new school when proof of attendance is received.
Financial matters									
Annual accounts	Personal* / Financial Data	SBM	SAO/Bursar	On the School Network, (Finance Drive) and on Governor Hub when reported on.	Sound financial management	Public interest/official authority			Current year + 6 years
Purchase Orders, Invoices, Payments	Personal* / Financial Data	SBM	Head / Deputy	On the School Network, (Finance Drive) and on Governor Hub when reported on.	Sound financial management	Public interest/official authority			Current year + 6 years
Records around budget management	Personal* / Financial Data	SBM	Site manager / Bursar / SAO?	On the School Network, (Finance Drive) and on Governor Hub when reported on.	Sound financial management	Public interest/official authority			Current year + 6 years
Asset management	Personal* / Financial Data	SBM	Site manager / Bursar / SAO?	On the School Network, (Finance Drive) and on Governor Hub when reported on.	Sound financial management	Public interest/official authority			Current year + 6 years
School Fund	Personal* / Financial Data	SBM	Bursar / Head / SAO	On the School Network, (Finance Drive) and on Governor Hub when reported on.	Sound financial management	Public interest/official authority			Current year + 6 years

FSM* - free school meals registers	Personal* / Financial Data	SBM	Bursar / Head / SAO	Individual information is secured within the pupil's personal file. General data (anonymised) shared wider including on website.	Sound financial management	Public interest/official authority			Registers: Current year + 6 years, Personal Data: personal file.
School meals registers	Personal* / Financial Data	SBM	Bursar / Head / SAO	Anonymised data shared with Catering	Sound financial management	Public interest/official authority			Current year + 6 years
Records relating to school lettings	Personal* / Financial Data	SBM	Bursar / Head / SAO	On the School Network, (Finance Drive) and on Governor Hub when reported on.	Sound financial management	Public interest/official authority			Current year + 6 years
Records relating to school maintenance	Personal* / Financial Data	SBM	Bursar / Head / SAO	On the School Network, (Finance Drive) and on Governor Hub when reported on.	Sound financial management	Public interest/official authority			Current year + 6 years
Access control / passwords* into systems									
Authorise data access / Nominated Contacts	Personal* Data	Headteacher/Deputy	Head	Turniton as network manager	Access to system(s)	Public interest/official authority			Until changes in personnel or in-line with password policy
Password to DfE or LA systems	Personal* Data	Headteacher/Deputy	Head / SAO	SMT only	Access to system(s)	Public interest/official authority			Until changes in personnel or in-line with password policy
Network administration / password lists	Personal* Data	Headteacher/Deputy	Network Manager / Support Provider	Turniton and SLT	Access to system(s)	Public interest/official authority			Until changes in personnel or in-line with password policy
USO password information	Personal* Data	Headteacher/Deputy	USO Nominated contacts	Turniton and SLT	Access to system(s)	Public interest/official authority			Until changes in personnel or in-line with password policy
Email management	Personal* Data	Headteacher/Deputy	USO Nominated contacts	Turniton and SLT	Access to system(s)	Public interest/official authority			Until changes in personnel or in-line with password policy
Web filtering management	Personal* Data	Headteacher/Deputy	USO Nominated contacts	Turniton and SLT	Access to system(s)	Public interest/official authority			Until changes in personnel or in-line with password policy
School website administration	Personal* Data	Headteacher/Deputy	Designed staff?	Turniton and SLT	Access to system(s)	Public interest/official authority			Until changes in personnel or in-line with password policy

Social media platforms, e.g. Twitter	Personal* Data	Headteacher/Deputy	Designed staff?	Turniton and SLT	Access to system(s)	Public interest/official authority			Until changes in personnel or in-line with password policy
Learning Platform password information	Personal* Data	Headteacher/Deputy	USO Nom Con / MLE Key teacher	Turniton and SLT. Some Class Teachers where applicable.	Access to system(s)	Public interest/official authority			Until changes in personnel or in-line with password policy
Communications									
Information added to website	Unrestricted (public)	Headteacher/Deputy	Designated website administrators	Via E4 Education website.	Business Continuity / communication	Public interest/official authority			Until changes in personnel or in-line with password policy
Information added to social media	Unrestricted (public)	Headteacher/Deputy	Designated social media administrators	Not currently using	Business Continuity / communication	Explicit consent	Not currently using. Personal data would never be shared through this method.	Not currently using.	Until changes in personnel or in-line with password policy
Learning Platform content	Unrestricted (public)	Headteacher/Deputy	Designated LP lead and deputy	Within the platform.	Teaching and Learning /statutory returns	Public interest/official authority			Until changes in personnel or in-line with password policy
Parental messaging system correspondence	Unrestricted (public)	Headteacher/Deputy	Head / Deputy / SAO	Via E4 Education website.	Business Continuity / communication	Public interest/official authority			System removes pupils who come off roll automatically (same day)
USO School Open Check	Unrestricted (public)	Headteacher/Deputy	SAO/ Head / Deputy / Nom Con	Within LGfL services.	Business Continuity / communication	Public interest/official authority			System removes staff and pupils who come off roll /eave employment automatically (same day)
Back-up media (where on site)	Special Categories of Personal Data*	Headteacher/Deputy	SAO / Network manager / technician	Standalone backup devices.	Business Continuity / communication	Public interest/official authority			Daily backup with 3-day rotation
Back-up media in Cloud	Special Categories of Personal Data*	Headteacher/Deputy	LGfL / Network manager / technician	Within the services specified, e.g. Office 365	Business Continuity / communication	Public interest/official authority			Daily backup with 3-day rotation
Emergency mobile phone loaded with data	Special Categories of Personal Data*	Headteacher/Deputy	Head / Deputy / SAO	Not currently using	Business Continuity / communication	Public interest/official authority			N/A
Governors									

Governors' documents with sensitive content	Special Categories of Personal Data*	Chair of Governors	Head / SAO / Chair / SLT	Governor Hub and School Network	Business Continuity / communication	Public interest/official authority			Date of meeting + 10 years
Governors' standard published meeting documents	Unrestricted (public)	Chair of Governors	Head / SAO / Chair / SLT	Governor Hub and School Network	Business Continuity / communication	Public interest/official authority			Date of meeting + 6 years
Reports presented to Governors meeting	Special Categories of Personal Data*	Chair of Governors	Head / SAO / Chair / SLT	Governor Hub and School Network	Business Continuity / communication	Public interest/official authority			Date of meeting + 6 years
Annual governors reports	Unrestricted (public)	Chair of Governors	Head / SAO / Chair / SLT	Governor Hub and School Network	Business Continuity / communication	Public interest/official authority			Date of meeting + 10 years
Annual parents' meeting papers	Unrestricted (public)	Headteacher	Head / SAO / Chair / SLT	School Network	Business Continuity / communication	Public interest/official authority			Date of meeting + 6 years
Policies and plans administered by Governing body	Unrestricted (public)	Chair of Governors	Head / SLT / specialist teachers	Governor Hub and School Network	Business Continuity / communication	Public interest/official authority			Life of policy + 3 years
Other T&L potentially sensitive material									
Student photos* (not required for pupil record)	Personal* Data	Headteacher	Class teachers	School Network	Teaching and learning /statutory returns	Explicit consent	When student joins roll.	New School Starter Booklet filled in and stored as hard copy. SIMS updated with details.	Relevant life of the photo / annual house-keeping within 6 years
Staff photos* (not required for Personal record)	Personal* Data	Various	SAO/office administrators / staff	School Network	Business Continuity / communication	Explicit consent	When photos are taken.	Staff offered choice of photos. Consent	Relevant life of the photo / annual house-keeping
Pupil work, e.g. Class Books	Personal* Data	Various	Class teachers	Hardcopies of work stored in books in each class and often scanned work saved on School Network	Teaching and Learning /statutory returns	Public interest/official authority			Pupil books retained for one full term after the year of use.
Pupil work for qualifications, e.g.	Personal* Data	Various	Class teachers	Hardcopies of work stored in books, some typed assessments	Teaching and Learning	Public interest/official authority			Year 10 pupil work retained for Year 11 plus for one full term after the year of use.

GCSE Coursework				and scanned work saved on School Network	/statutory returns				
Student reports (not in core MIS)	Special Categories of Personal Data*	Headteacher/Deputy	Class teachers	School Network	Teaching and Learning /statutory returns	Public interest/official authority			part of pupil record
Student assessments (not in core MIS)	Special Categories of Personal Data*	Class Teachers	Class teachers	Bsquared and in Spreadsheets on School Network	Teaching and Learning /statutory returns	Public interest/official authority			part of pupil record
Third Party comparative performance data	Unrestricted (public)	Headteacher/Deputy	Head / SLT /Governors	On the specific platform, e.g GL Assessment.	Teaching and Learning /statutory returns	Public interest/official authority			part of pupil record
Other operational potentially sensitive material									
CCTV saved footage	Special Categories of Personal Data*	Headteacher	Third Party support / SLT?	Backed up on site.	Safeguarding / Security	Public interest/official authority			Minimum 30 day read/re-write cycle
Visitor signing-in book / management system	Special Categories of Personal Data*	SBM	Office staff / Third Party support?	InVentory sign-in system	Safeguarding / Security	Public interest/official authority			Current year + 6 years / review
Newsletters and information with a short operational life	Unrestricted (public)	Headteacher	Designated staff	School Network and Website	Business Continuity / communication	Public interest/official authority	May require consent if containing photos	Consent will be sought and stored individually.	3 years from issue