Langley Grammar School

Data Protection Policy
September 2025

1. Rationale and aims

In order to function properly, the school is required to process personal information about staff, students and other individuals who come into contact with school. We are also obliged to collect and use data to fulfil our obligations to the Local Authority, Department for Education and other bodies. We regard the lawful and correct treatment of personal information as very important to successful operations, and to maintaining confidence between ourselves and those with whom we deal. We are conscious that some of the personal data we hold is classified as sensitive data and are aware of the extra care this kind of information requires.

We aim to ensure that all personal data collected about staff, students, parents, governors, visitors and other individuals is collected, stored and processed in accordance with UK data protection law.

To this end this policy meets the requirements of legislation and relevant guidance, namely:

- The Data Protection Act 2018.
- Guidance published by the Information Commissioner's Office (ICO) on the GDPR and the ICO's code of practice for subject access requests.
- The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2020 (which incorporated EU GDPR into UK legislation with some amendments)
- The requirements of the Protection of Freedoms Act 2012 when referring to our use of biometric data.
- The ICO's code of practice for the use of surveillance cameras and personal information.

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

2. Data Protection Principles

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

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

This policy sets out how we aim to comply with these principles.

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

a) 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

b) The data needs to be processed so that the school can **comply with a legal obligation**

c) The data needs to be processed to ensure the **vital interests** of the individual e.g. to protect someone's life

d) 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

e) 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)

f) 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 data protection law.

3. Definitions

Term	Definition
Personal data	**Any information** relating to an identified individual. In addition to names, addresses and phone numbers, dates of birth etc, examples of personal data in a school context might include: • An email sent by one member of staff to another about a student • A print-out of a student's school report • Absence records relating to a member of staff • Performance management records • A list of contact details of parents given to a member of staff for an educational visit • A record of a return-to-work conversation • A comment posted on social media about an individual • DBS certificates • Parents' bank details for an online payment system • Counselling and safeguarding records • An email trail between a parent and member of staff regarding the progress of a student Personal data may include information specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity. Even if an individual is not specifically named, the information is still defined as personal data if the individual can still be identified, for example by: • The individual's initials • Location data (e.g. his or her address) • An online identifier, such as a username

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. The Data Controller

The 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.

5. Roles and responsibilities

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

Governing Board

- 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 (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. The DPO will, as appropriate, report on data protection issues to the Governing Board and Headteacher and act as the first point of contact for individuals whose data the school processes, and for the ICO.

Headteacher

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

All staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy and following the expectations set out in Appendix 4.
- Informing the school of any changes to their personal data, such as a change of address.
- Only processing personal data where it is necessary in order to do their jobs.
- Keeping data accurate and, where necessary, up to date. [Inaccurate data will be rectified or erased when appropriate].
- Deleting or anonymising personal data when it is no longer needed, in accordance with the school's record retention schedule.
- 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 or ICO defined adequacy-recognised territories
    - If there has been a data breach or a potential data breach
    - Whenever they are engaging in a new activity that may affect the privacy rights of individuals
    - If they need help with any contracts or sharing personal data with third parties

6. Sharing personal data

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

a) There is an issue with a student or parent/carer that puts the safety of our staff at risk

b) We need to liaise with other agencies – we will seek consent as necessary before doing this

c) Our suppliers or contractors need data to enable us to provide services to our staff and students – for example, IT companies, educational visit providers. 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 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 students 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 and will take into account the latest guidance from the ICO related to specific territories.

7. Data protection impact assessments

We will complete data protection impact assessments where the school's processing of personal data presents a high risk to rights and freedoms of individuals, and where appropriate, when introducing new technologies.

8. 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.

If staff receive a subject access request they must immediately forward it to the DPO. The procedure for responding to subject access requests is set out in Appendix 1.

9. Other data protection rights of the individual

In addition to the right to make a subject access request 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 ICO
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)

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

10. Biometric recognition systems

Where we use students' biometric data as part of an automated biometric recognition system (for example, sixth form students using finger prints to register their attendance) we will comply with the requirements of the Protection of Freedoms Act 2012.

Parents/carers will be notified before any biometric recognition system is put in place or before their child first takes part in it. 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 students have the right to choose not to use the school's biometric system(s). We will provide alternative means of accessing the relevant services for those students. Parents/carers and students 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 student 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 student's parent(s)/carer(s).

11. Photographs and videos

As part of our school activities, we may take photographs and record video images of individuals within our school. We will obtain written consent from parents/carers, or students aged 18 and over, for photographs and videos to be taken of students for communication, marketing and promotional materials.

Where we need parental consent, we will clearly explain how the photograph and/or video will be used to both the parent/carer and student. Where we do not require parental consent, we will clearly explain to the student how the photograph and/or video will be used.

Uses may include but are not restricted to the following:

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

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

When using photographs and videos externally or sharing online we will not accompany them with information about the child that could result in them being identified.

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

12. CCTV

We use CCTV in various locations around the school site to ensure the safety and well-being of staff, students, visitors and for reasons of site security. 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 will make it clear where individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use.

13. Artificial Intelligence (AI)

Artificial intelligence (AI) tools are increasingly widespread and accessible. Staff, students and parents/carers may be familiar with generative platforms such as ChatGPT, Microsoft Copilot, or similar services. While AI has potential educational benefits, it also presents risks to sensitive and personal data.

To protect individuals' privacy and to remain compliant with data protection law:

- Personal or sensitive data must not be entered into any unauthorised AI tools or platforms.
- Students must not use generative AI tools for school work unless this has been explicitly approved by the Senior Leadership Team and appropriate safeguards are in place.
- Original student work must not be used to train AI models unless consent has been gained.

Any proposed use of AI systems within the school must be risk-assessed, and where necessary a Data Protection Impact Assessment will be completed before adoption.

14. 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 3.

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 students 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 students
- A student gaining access to a member of staff's Office 365 credentials and downloading and forwarding emails containing personal information on a data subject

15. Data security and storage of records

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

In particular:

- Papers containing sensitive personal data (for example, counselling records, SEN and health information, parents' personal contact details) must be kept securely (for example in a locked cupboard, desk, office or filing cabinet).
- Papers containing less sensitive personal data (for example, students' assessment results) should not be on display. For example, they should not be left lying around on teachers' desks in classrooms, pinned to notice/display boards, nor left anywhere else where there is general access. Such information should be filed away out of sight.
- Unencrypted memory sticks (flash drives), external hard drives or similar must never be used to store personal data, and the use of memory sticks and external drives is generally discouraged.
- Reasonable steps should be taken to ensure that portable devices (for example laptops, iPads) containing personal data are kept securely when taken out of school.
- Paper documents containing personal data, sensitive or otherwise, (e.g. medical information, contact details (other than school email addresses), students' assessment results, SEN information) must be shredded when finished with, rather than placed in recycling or waste paper bins.
- 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.
- Passwords that enable access to websites or systems containing personal data (for example Office 365, the school network, SIMS) must not be written down or disclosed.

- Passwords that enable access to personal data, should, where possible, be sufficiently complex so they cannot be guessed easily and can resist 'brute force' attacks i.e. ideally be at least 8 characters long and include a mix of capital and lowercase letters, numbers and symbols.
- Passwords that enable access to websites or systems containing personal data should be changed at regular intervals.
- Staff must contact the DPO or the Data Manager for advice on procedures before sharing personal information with third parties (i.e. people beyond the school or other organisations).

16. Training

Staff will receive reminders and updates periodically of key data protection procedures and expectations. Data protection will also form part of continuing professional development, where changes to legislation, guidance or the school's processes make it necessary.

17. Privacy notices

Under data protection law, individuals have a right to be informed about how the school uses any personal data (information) that we hold about them. We comply with this right by providing 'privacy notices' (sometimes called 'fair processing notices') to individuals where we are processing their personal data. These are detailed in Appendix 2

Ratification and review dates

Reviewed by	**Headteacher & Resources Committee**	**Date**	**Sept 2025**
Approved by	**Governing Board**	**Date**	**Oct 2025**
Next Review	**School Business Manager & Headteacher**	**Date**	**Sept 2027**

Appendix 1 – Procedures for 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
- The safeguards provided if the data is being transferred internationally

Subject access requests should be made in writing to the school's Data Protection Officer and include:

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

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 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 students at our school may not be granted without the express permission of the student. This is not a rule and a student's ability to understand their rights will always be judged on a case-by-case basis.

When we disclose information to a child we understand that the importance of using language that the child is likely to be able to understand.

Responding to subject access requests

When responding to requests, we:

- May ask the individual to provide 2 forms of identification in order to confirm the identity of the data subject or their relationship to a child, where the child is the data subject.
- 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 irrespective of when the request is made
- 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
- Would include another person's personal data that we can't reasonably anonymise, and we don't have the other person's consent and it would be unreasonable to proceed without it
- Is part of certain sensitive documents, such as those related to crime, immigration, legal proceedings or legal professional privilege, management forecasts, negotiations, confidential references, or exam scripts

Responding to a subject access request may involve providing information that relates both to the individual making the request and to another individual. The DPA 2018 states that organisations do not have to comply with the request if it would mean disclosing information about another individual who can be identified from that information, except if:

- the other individual has consented to the disclosure; or
- it is reasonable to comply with the request without that individual's consent.

In determining whether it is reasonable to disclose the information, we are required to take into account all of the relevant circumstances, including:

- the type of information that you would disclose;
- any duty of confidentiality you owe to the other individual;
- any steps you have taken to seek consent from the other individual;
- whether the other individual is capable of giving consent; and
- any express refusal of consent by the other individual.

Reaching decisions on whether to disclose personal information about a third party involves balancing the data subject's right of access against the other individual's rights. However for the avoidance of doubt, we are not able to refuse to provide access to personal data about an individual simply because we obtained that data from a third party.

Grounds for refusing to act on a Subject Access Request

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. Also, 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.

Appendix 2 – Privacy Notices

Langley Grammar School

Privacy notice for parents/carers

Under data protection law, individuals have a right to be informed about how the school uses any personal data (information) that we hold about them. We comply with this right by providing 'privacy notices' (sometimes called 'fair processing notices') to individuals where we are processing their personal data.

This privacy notice explains how we collect, store and use personal information **about our students**.

Langley Grammar School, is a 'data controller' for the purposes of data protection law. Contact details for our Data Protection Officer can be found in section 13 'Contact us'.

1. What personal information do we hold?

Personal data that we may collect, use, store and (when appropriate) share about students includes, but is not limited to:

- contact details, contact preferences, date of birth, identification documents
- results of routine school assessments and externally set examinations
- characteristics such as ethnic background, eligibility for free school meals, or special educational needs
- records of exclusions and other information about behaviour
- details of any medical conditions, including physical and mental health
- attendance information
- safeguarding information
- details of any support received, including plans and support providers
- photographs
- CCTV images captured in school

We may also hold data about students that we have received from other organisations, including other schools, local authorities and the Department for Education.

2. Why do we use this information?

We use this data to:

- support students' learning and achievement
- monitor and report on student attainment and progress
- provide appropriate pastoral care and support
- protect and support students' welfare
- assess the quality of our provision
- administer admissions waiting lists
- carry out research, e.g. students' travel arrangements
- comply with the law regarding data sharing

3. What is our legal basis for using this information?

We only collect and use students' personal data when the law allows us to. Most commonly, we process it where:

- we need to comply with a legal obligation, or
- we need it to perform an official task in the public interest

We may also process students' personal data in situations where:

- we have obtained consent to use it in a certain way, or
- we need to protect the individual's vital interests (or someone else's interests)

Where we have obtained consent to use students' personal data, this consent can be withdrawn at any time. We will make this clear when we ask for consent and explain how consent can be withdrawn.

Some of the reasons listed for collecting and using students' personal data overlap, and there may be several grounds which justify our use of this data.

4. How do we collect this information?

The majority of information we collect about students is mandatory; however, there is some information that can be provided voluntarily. Whenever we seek to collect information from you or your child, we make it clear whether providing it is mandatory or optional. If it is mandatory, we will explain the possible consequences of not complying.

5. How do we store this information?

We keep personal information about students while they are attending the school. We may also keep it after they have left the school if this is necessary in order to comply with our legal obligations. Our record retention schedule sets out how long we keep information about students. Information may be stored on our school computer systems or on paper.

6. Information sharing

We do not share information about students with any third party without consent unless the law and our policies allow us to do so. Where it is legally required, or necessary (and it complies with data protection law) we may share personal information about students with:

- relevant local authorities – to meet our legal obligations to share certain information such as safeguarding concerns and exclusions
- the Department for Education
- students' families and representatives
- educators and examining bodies
- Ofsted
- suppliers and service providers – to enable them to provide the service we have contracted them for
- financial organisations
- central and local government
- our auditors
- survey and research organisations

- health authorities and health or social welfare organisations
- security organisations
- professional advisers and consultants
- charities and voluntary organisations
- police forces, courts, tribunals
- online platforms with cloud storage, such as School Cloud, ClassCharts and Microsoft 365.
- organisations that we work with to deliver educational experiences as part of our educational visits and enrichment provision.
- other professional bodies

7. National Pupil Database

We are required to provide information about our students to the Department for Education as part of statutory data collections such as the school census.

Some of this information is then stored in the National Pupil Database (NPD), which is owned and managed by the Department and provides evidence on school performance to inform research. The database is held electronically so it can easily be turned into statistics. The information is securely collected from a range of sources including schools, local authorities and exam boards.

The Department for Education may share information from the NPD with other organisations which promote children's education or wellbeing in England. Such organisations must agree to strict terms and conditions about how they will use the data.

For more information, see the Department's webpage on how it collects and shares research data.
You can also contact the Department for Education with any further questions about the NPD.

8. Youth support services

Once our students reach the age of 13, we are legally required to pass on certain information about them to Slough Borough Council and other local authorities as they have legal responsibilities regarding the education or training of 13-19 year-olds. This information enables the local authorities to provide youth support services, post-16 education and training services, and careers advisers.

Parents/carers, or students once aged 16 or over, can contact our data protection officer to request that we only pass the individual's name, address and date of birth to the local authorities.

9. Transferring data internationally

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

Where we share data with third parties who process data within the United States of America, the school will ensure that the US entity is certified under the UK extension to the EU–US Data Privacy Framework, and that such transfers comply with the latest ICO guidance.

There are a small number of third parties that we share personal data with who then go on to process these data in the USA including:

- Apple – eg we share data on students' names, Apple IDs and students' work stored on various applications.

- LIBF and Trinity College London – we provide information about students to these two examination boards so they can assess and accredit students' work for two of our enrichment programmes.

We will continue to share data with these organisations unless the ICO rules that doing so is no longer compliant with relevant legislation in the UK.

10. Parents' and students' rights regarding personal data

Individuals have a right to make a **'subject access request'** to gain access to personal information that the school holds about them. Parents/carers can make a request with respect to their child's information where the child is not considered mature enough to understand their rights over that information (usually under the age of 12), or where the child has provided consent. Parents also have the right to make a subject access request with respect to any personal information the school holds about them.

If you make a subject access request, and if we do hold information about you or your child, we will:

- give you a description of the information we hold
- tell you why we are holding and processing it, and how long we will keep it for
- explain where we got it from, if not from you or your child
- tell you who it has been, or will be, shared with
- let you know whether any automated decision-making is being applied to the data, and any consequences of this
- give you a copy of the information in an understandable form

Individuals also have the right for their personal information to be transmitted electronically to another organisation in certain circumstances.

If you would like to make a request, please contact our data protection officer.

Langley Grammar School is an academy. Parents/carers of children educated in schools with academy status do **not** have the legal right to access to their child's **educational record**. However, we are willing to allow parents access to that record in line with their rights in maintained schools. To request access, please contact our Data Protection Officer. A charge may be applied to cover the administrative costs of providing this information.

11. Other rights

Under data protection law, individuals have certain rights regarding how their personal data is used and kept safe, including the right to:

- object to the use of personal data if it would cause, or is causing, damage or distress
- prevent it being used to send direct marketing
- object to decisions being taken by automated means (by a computer or machine, rather than by a person)
- in certain circumstances, have inaccurate personal data corrected, deleted or destroyed, or restrict processing
- claim compensation for damages caused by a breach of the data protection regulations

To exercise any of these rights, please contact our Data Protection Officer.

12. Complaints

We take any complaints about our collection and use of personal information very seriously. If you think that our collection or use of personal information is unfair, misleading or inappropriate, or have any other concern about our data processing, please raise this with us in the first instance.

To make a complaint, please contact our Data Protection Officer.

Alternatively, you can make a complaint to the Information Commissioner's Office:

- Report a concern online at https://ico.org.uk/concerns/
- Call 0303 123 1113
- Or write to: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

13. Contact us

If you have any questions, concerns or would like more information about anything mentioned in this privacy notice, please contact our Data Protection officer:

- Mr Gary Botha, Business Manager
- 01753 598300
- school@lgs.slough.sch.uk

This notice is based on the Department for Education's model privacy notice for students, amended for parents and to reflect the way we use data in this school.

Langley Grammar School

Privacy notice for students

You have a legal right to be informed about how our school uses any personal information that we hold about you. To comply with this, we provide a 'privacy notice' to you where we are processing your personal information.

This privacy notice explains how we collect, store and use personal information about **you**. Langley Grammar School, is the 'data controller' for the purposes of data protection law. Contact details for our Data Protection Officer can be found in section 13 'Contact us'.

1. What personal data do we hold?

We hold some personal information about you to make sure we can help you learn and to look after you at school. For the same reasons, we get information about you from some other places too – like other schools, the local council and the government.

This information includes:

- your contact details
- assessment and examination results
- your attendance records
- any characteristics, such as your ethnic background or any special educational needs
- any medical conditions you have
- details of any behaviour issues or exclusions
- photographs
- audio and video recordings of lessons, which may capture the actions and contributions made by you and others.
- CCTV images

2. Why do we use this information?

We use this data to help run the school, including to:

- contact you and your parents when we need to
- check how you're doing in exams and work out whether you or your teachers need any extra help
- track how well the school as a whole is performing
- provide education to you and/or other students who are unable to be in lessons
- investigate any behaviour or safeguarding issues and apply rewards and sanctions in line with our behaviour for learning policy
- support your wellbeing

Data from video and audio recordings of lessons may be shared with other students in your class or year group, and with other staff across the school.

3. What is our legal basis for using this data?

We will only collect and use your information when the law allows us to. Most often, we will use your information where:

- we need to comply with the law, or
- we need to use it to carry out a task 'in the public interest' - eg in order to provide you with an education

Sometimes, we may also use your personal information where:

- you, or your parents/carers have given us permission to use it in a certain way, or
- we need to protect your interests, or someone else's interest

Where we have permission to use your data, you or your parents may withdraw this at any time. We will make this clear when we ask for permission and explain how to go about withdrawing consent.

Some of the reasons listed above for collecting and using your information overlap, and there may be several grounds which mean we can use your data.

4. Collecting this information

While in most cases you, or your parents/carers, must provide the personal information we need to collect, there are some occasions when you can choose whether or not to provide the data.

We will always tell you if it's optional. If you must provide the data, we will explain what might happen if you don't.

5. How do we store this data?

We will keep personal information about you while you are a student at our school. We may also keep it after you have left the school, where we are required to by law.

We have a record retention schedule on our school website which sets out how long we must keep information about you. Information may be stored on our school computer systems, cloud servers within the UK or on paper.

Video and audio recordings of lessons and other teaching sessions are stored on our Office 365 platform on Microsoft's servers in the UK.

6. Data sharing

We do not share personal information about you with anyone outside the school without permission from you or your parents/carers, unless the law and our policies allow us to do so.

Where it is legally required, or necessary for another reason allowed under data protection law, we may share personal information about you with:

- local authorities such as Slough Borough Council – this is to meet our legal duties to share certain information such as concerns about students' safety and exclusions
- the Department for Education (a government department)
- your family and representatives
- educators and examining bodies
- Ofsted

- suppliers and service providers – so that they can provide the services we are paying them for
- financial organisations
- central and local government
- our auditors
- survey and research organisations
- health authorities, health and social welfare organisations
- security organisations
- professional advisers and consultants
- charities and voluntary organisations
- police forces, courts, tribunals
- online platforms with cloud storage, such as School Cloud, ClassCharts, and Microsoft 365.
- organisations that we work with to deliver educational experiences as part of our educational visits and enrichment provision.
- other professional bodies

7. National Pupil Database

We are required to provide information about you to the Department for Education as part of data collections such as the school census.

Some of this information is then stored in the National Pupil Database, which is managed by the Department for Education and provides evidence on how schools are performing to inform research. The database is held electronically so it can easily be turned into statistics. The information it holds is collected securely from schools, local authorities, exam boards and others.

The Department for Education may share information from the database with other organisations which promote children's education or wellbeing in England. These organisations must agree to strict terms and conditions about how they will use your data.

You can find more information about this on the Department for Education's webpage on how it collects and shares research data. You can also contact the Department for Education if you have any questions about the database.

8. Youth support services

Once you reach the age of 13, we are legally required to pass on certain information about you to Slough Borough Council or other local authorities as they have legal responsibilities regarding the education or training of 13-19 year olds.

This information enables them to provide youth support services, post-16 education and training services, and careers advisers. Your parents/carers, or you once you're 16, can contact our Data Protection Officer to ask us to only pass on your name, address and date of birth to the local authorities.

9. Transferring data internationally

Where we share data with an organisation that is based outside the European Economic Area, we will protect your data by following data protection law.

Where we share data with third parties who process data within the United States of America, the school will ensure that the US entity is certified under the UK extension to the EU–US Data Privacy Framework, and that such transfers comply with the latest ICO guidance.

There are a small number of third parties that we share personal data with who then go on to process these data in the USA including:

- Apple – eg we share data on students' names, Apple IDs and students' work stored on various applications.
- LIBF and Trinity College London – we provide information about students to these two examination boards so they can assess and accredit students' work for two of our enrichment programmes.

We will continue to share data with these organisations unless the ICO rules that doing so is no longer compliant with relevant legislation in the UK.

10. Your rights

How to access personal information we hold about you

You can find out if we hold any personal information about you, and how we use it, by making a **'subject access request'**, provided we judge that you can properly understand your rights and what they mean.

If we do hold information about you, we will:

- give you a description of it
- tell you why we are holding and using it, and how long we will keep it for
- explain where we got it from, if not from you or your parents
- tell you who it has been, or will be, shared with,
- let you know if we are using your data to make any automated decisions (decisions being taken by a computer or machine, rather than by a person)
- give you a copy of the information

You may also ask us to send your personal information to another organisation electronically in certain circumstances.

If you want to make a subject access request please contact our Data Protection Officer.

Your other rights over your data

You have other rights over how your personal data is used and kept safe, including the right to:

- say that you don't want it to be used if this would cause, or is causing, harm or distress
- stop it being used to send you marketing materials
- say that you don't want it used to make automated decisions (decisions made by a computer or machine,
- rather than by a person)
- have it corrected, deleted or destroyed if it is wrong, or restrict our use of it
- claim compensation if the data protection rules are broken and this harms you in some way

11. Complaints

We take any complaints about how we collect and use your personal information very seriously, so please let us know if you think we've done something wrong. You can make a complaint at any time by contacting our data protection officer. You can also complain to the Information Commissioner's Office in one of the following ways:

- Report a concern online at https://ico.org.uk/concerns/
- Call 0303 123 1113
- Or write to: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

12. Contact us

If you have any questions, concerns or would like more information about anything mentioned in this privacy notice, please contact our Data Protection Officer:

- Mr G Botha, Business Manager
- 01753 598300
- garybotha@lgs.slough.sch.uk

This notice is based on the Department for Education's model privacy notice for students, amended to reflect the way we use data in this school.

Langley Grammar School

Privacy notice for staff

Under data protection law, individuals have a right to be informed about how the school uses any personal information that we hold about them. We comply with this right by providing 'privacy notices' (sometimes called 'fair processing notices') to individuals where we are processing their personal information.

This privacy notice explains how we collect, store and use personal information about individuals we employ, or otherwise engage, to work at our school. Langley Grammar School is the 'data controller' for the purposes of data protection law.

This notice is based on the Department for Education's model privacy notice for the school workforce, amended to reflect the way we use data in this school.

1. What personal information do we hold?

We process data relating to those we employ, or otherwise engage, to work at our school. Personal data that we may collect, use, store and share (when appropriate) about you includes, but is not restricted to:

- contact details
- date of birth, marital status and gender
- next of kin and emergency contact numbers
- salary, annual leave, pension and benefits information
- bank account details, payroll records, National Insurance number and tax status information
- recruitment information, including copies of right to work documentation, references and other information included in a CV or cover letter or as part of the application process
- qualifications and employment records, including work history, job titles, working hours, training records and professional memberships
- performance management information
- outcomes of any disciplinary and/or grievance procedures
- absence data
- copy of driving licence
- photographs
- audio and video recordings of lessons, which may capture the actions and contributions made by you and others.
- CCTV footage
- data about your use of the school's IT systems

We may also collect, store and use information about you that falls into "special categories" of more sensitive personal data. This may include information about, for example:

- race, ethnicity and religious beliefs
- trade union membership
- health, including any medical conditions, and sickness records

2. Why do we use this information?

The purpose of processing this data is to help us run the school, including to:

- enable you to be paid
- facilitate safe recruitment, as part of our safeguarding obligations towards students
- support effective performance management
- inform our recruitment and retention policies
- allow better financial modelling and planning
- enable ethnicity and disability monitoring
- improve the management of workforce data across the sector
- support staff professional development
- provide education to students who are unable to be in lessons
- monitor and quality-assure the education that we provide
- investigate any behaviour or safeguarding issues amongst students and the professional conduct of staff
- support the work of the School Teachers' Review Body

Data from video and audio recordings of lessons may be shared with students in your class or year group, and with other staff across the school.

3. What is our lawful basis for using this information?

We only collect and use personal information about you when the law allows us to. Most commonly, we use it where we need to:

- fulfil a contract we have entered into with you
- comply with a legal obligation
- carry out a task in the public interest

Less commonly, we may also use personal information about you where:

- you have given us consent to use it in a certain way
- we need to protect your vital interests (or someone else's interests)
- we have legitimate interests in processing the data

Where you have provided us with consent to use your information, you may withdraw this consent at any time. We will make this clear when requesting your consent and explain how you go about withdrawing consent if you wish to do so.

Some of the reasons listed above for collecting and using personal information about you overlap, and there may be several grounds which justify the school's use of your information.

4. Collecting this information

While the majority of information we collect from you is mandatory, there is some information that you can choose whether or not to provide to us. Whenever we ask for information from you, we will make it clear whether you must provide this information (and if so, what the possible consequences are of not complying), or whether you have a choice.

5. How we store this data

We create and maintain an employment file for each staff member. The information contained in this file is kept secure and is only used for purposes directly relevant to your employment. Once your employment with us has ended, we will retain this file and delete the information in it in accordance with our record retention schedule. A copy of our record retention schedule can be obtained on request from our Data Protection Officer.

Information may be stored on our school computer systems, cloud servers within the UK or on paper. Video and audio recordings of lessons and other teaching sessions are stored on our Office 365 platform on Microsoft's servers in the UK.

6. Data sharing

We do not share information about you with any third party without your consent unless the law and our policies allow us to do so. Where it is legally required, or necessary (and it complies with data protection law) we may share personal information about you with:

- Slough Borough Council or other local authorities – to meet our legal obligations to share certain information with it, such as safeguarding concerns
- the Department for Education
- your family or representatives
- educators and examining bodies
- Ofsted
- suppliers and service providers – to enable them to provide the service we have contracted them for
- financial organisations
- central and local government
- our auditors
- survey and research organisations
- trade unions and associations
- health authorities, health and social welfare organisations
- security organisations
- professional advisers and consultants
- charities and voluntary organisations
- police forces, courts, tribunals
- online platforms with cloud storage, such as School Cloud, ClassCharts, and Microsoft Office 365.
- other schools, employment and recruitment agencies, other professional bodies

7. Transferring data internationally

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.

Where we share data with third parties who process data within the United States of America, the school will ensure that the US entity is certified under the UK extension to the EU–US Data Privacy Framework, and that such transfers comply with the latest ICO guidance.

There are a small number of third parties that we share personal data with who then go on to process these data in the United States of America. We will continue to share data with these organisations unless the ICO rules that doing so is no longer compliant with relevant legislation in the UK.

8. Your rights

How to access personal information we hold about you

Individuals have a right to make a **'subject access request'** to gain access to personal information that the school holds about them.

If you make a subject access request, and if we do hold information about you, we will:

- give you a description of it
- tell you why we are holding and processing it, and how long we will keep it for
- explain where we got it from, if not from you
- tell you who it has been, or will be, shared with
- let you know whether any automated decision-making is being applied to the data, and any consequences of this
- give you a copy of the information in an intelligible form

You may also have the right for your personal information to be transmitted electronically to another organisation in certain circumstances.

If you would like to make a subject access request, please contact our Data Protection Officer.

Your other rights regarding your data

Under data protection law, individuals have certain rights regarding how their personal data is used and kept safe. You have the right to:

- object to the use of your personal data if it would cause, or is causing, damage or distress
- prevent your data being used to send direct marketing
- object to the use of your personal data for decisions being taken by automated means (by a computer or machine, rather than by a person)
- in certain circumstances, have inaccurate personal data corrected, deleted or destroyed, or restrict processing
- claim compensation for damages caused by a breach of the data protection regulations

To exercise any of these rights, please contact our Data Protection Officer.

9. Complaints

We take any complaints about our collection and use of personal information very seriously. If you think that our collection or use of personal information is unfair, misleading or inappropriate, or have any other concern about our data processing, please raise this with us in the first instance.

To make a complaint, please contact our **Data Protection Officer**.

Alternatively, you can make a complaint to the Information Commissioner's Office:

- Report a concern online at https://ico.org.uk/concerns/
- Call 0303 123 1113
- Write to: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

10. Contact us

If you have any questions, concerns or would like more information about anything mentioned in this privacy notice, please contact our **Data Protection Officer**:

- Gary Botha, Business Manager
- 01753 598300
- garybotha@lgs.slough.sch.uk

Langley Grammar School

Privacy notice for governors/trustees

Under data protection law, individuals have a right to be informed about how the school uses any personal information that we hold about them. We comply with this right by providing 'privacy notices' (sometimes called 'fair processing notices') to individuals where we are processing their personal information.

This privacy notice explains how we collect, store and use personal information about governors and volunteers. Langley Grammar School is the 'data controller' for the purposes of data protection law.

This notice is based on the both model privacy notice for governors and trustees from the Department for Education and The Key, amended to reflect the way we use data in this school.

1. What personal information do we hold?

We process data relating to governors and volunteers. Personal data that we may collect, use, store and share (when appropriate) about you includes, but is not restricted to:

- contact details
- date of birth, marital status and gender
- next of kin and emergency contact numbers
- personal financial information, including bank account details
- information needed to perform DBS and Section 128 checks,
- Information about business and pecuniary interests
- Background information on qualifications and career history
- Records of training completed and contributions at meetings
- outcomes of any disciplinary and/or grievance procedures
- photographs
- data about use of the school's IT systems

We may also collect, store and use information about you that falls into "special categories" of more sensitive personal data. This may include information about, for example:

- Information about any health conditions, disabilities and access arrangements you have identified that we need to be aware of
- CCTV footage

2. Why do we use this information?

The purpose of processing this data is to help us run the school, including to:

- Establish and maintain effective governance
- Meet statutory obligations for publishing and sharing governors'/trustees' details
- Facilitate safe recruitment, as part of our safeguarding obligations towards pupils
- Undertake equalities monitoring

- Ensure that appropriate access arrangements can be provided for volunteers who require them
- Make sure our information and communication systems, equipment and facilities (e.g. school computers) are used appropriately, legally and safely

3. What is our lawful basis for using this information?

We only collect and use personal information about you when the law allows us to. Most commonly, we use it where we need to:

- comply with a legal obligation
- fulfil the obligations of a contract
- carry out a task in the public interest

Less commonly, we may also use personal information about you where:

- you have given us consent to use it in a certain way
- we need to protect your vital interests (or someone else's interests)
- we have legitimate interests in processing the data

Where you have provided us with consent to use your information, you may withdraw this consent at any time. We will make this clear when requesting your consent and explain how you go about withdrawing consent if you wish to do so.

Some of the reasons listed above for collecting and using personal information about you overlap, and there may be several grounds which justify the school's use of your information.

4. Collecting this information

We will only collect and use your data when the law allows us to. While the majority of information we collect from you is mandatory, there is some information that you can choose whether or not to provide to us. Whenever we ask for information from you, we will make it clear whether you must provide this information (and if so, what the possible consequences are of not complying), or whether you have a choice.

5. How we store this data

We hold data securely for the set amount of time shown in our data retention schedule. A copy of our record retention schedule can be obtained on request from our Data Protection Officer.

Information may be stored on our school computer systems, cloud servers within the UK/EU or on paper. We have put in place appropriate security measures to prevent your personal information from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed.

We will dispose of your personal data securely when we no longer need it.

6. Data sharing

We do not share information about you with any third party without your consent unless the law and our policies allow us to do so. Where it is legally required, or necessary (and it complies with data protection law) we may share personal information about you with:

- Slough Borough Council or other local authorities – to meet our legal obligations to share certain information with it, such as safeguarding concerns

- the Department for Education
- your family or representatives
- Ofsted
- suppliers and service providers – to enable them provide the service we have contracted them for
- financial organisations
- central and local government
- our auditors
- survey and research organisations
- trade unions and associations
- health authorities, health and social welfare organisations
- security organisations
- professional advisers and consultants
- charities and voluntary organisations
- police forces, courts, tribunals
- online platforms with cloud storage, such as School Cloud, ClassCharts, and Microsoft Office 365.

Providing governors personal information to suppliers of banking services and Companies House

Irrespective of legislation allowing us to share your personal information with third parties without consent in specific circumstances, we will only share your personal information with providers of financial services or Companies House after first consulting with you.

In such circumstances, we will:

- inform you in writing of the intention to share the information
- provide you with a copy of the personal data that we intend to share
- explain the reason for intending to share the information and in particularly whether we are required to do so.

We will then provide you with a reasonable opportunity to reply so that you may:

- check and if necessary correct that the information to be shared is accurate
- object to the information being shared.

If you inform us that information to be shared is inaccurate, we will correct it before sharing it and provide you with a copy of the information that is to be shared. Where you object to the information being shared, we will seek to reach agreement with you, recognising your rights as a data subject and the School's obligations to share information in particular circumstances.

7. Transferring data internationally

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.

Where we share data with third parties who process data within the United States of America, the school will ensure that the US entity is certified under the UK extension to the EU–US Data Privacy Framework, and that such transfers comply with the latest ICO guidance.

There are a small number of third parties that we share personal data with who then go on to process these data in the United States of America. We will continue to share data with these organisations unless the ICO rules that doing so is no longer compliant with relevant legislation in the UK.

8. Your rights

How to access personal information we hold about you

Individuals have a right to make a **'subject access request'** to gain access to personal information that the school holds about them.

If you make a subject access request, and if we do hold information about you, we will:

- give you a description of it
- tell you why we are holding and processing it, and how long we will keep it for
- explain where we got it from, if not from you
- tell you who it has been, or will be, shared with
- let you know whether any automated decision-making is being applied to the data, and any consequences of this
- give you a copy of the information in an intelligible form

You may also have the right for your personal information to be transmitted electronically to another organisation in certain circumstances.

If you would like to make a subject access request, please contact our Data Protection Officer.

Your other rights regarding your data

Under data protection law, individuals have certain rights regarding how their personal data is used and kept safe. You have the right to:

- object to the use of your personal data if it would cause, or is causing, damage or distress
- prevent your data being used to send direct marketing
- object to the use of your personal data for decisions being taken by automated means (by a computer or machine, rather than by a person)
- in certain circumstances, have inaccurate personal data corrected, deleted or destroyed, or restrict processing
- claim compensation for damages caused by a breach of the data protection regulations

To exercise any of these rights, please contact our Data Protection Officer.

9. Complaints

We take any complaints about our collection and use of personal information very seriously. If you think that our collection or use of personal information is unfair, misleading or inappropriate, or have any other concern about our data processing, please raise this with us in the first instance.

To make a complaint, please contact our **Data Protection Officer**.

Alternatively, you can make a complaint to the Information Commissioner's Office:

- Report a concern online at https://ico.org.uk/concerns/
- Call 0303 123 1113
- Write to: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

10. Contact us

If you have any questions, concerns or would like more information about anything mentioned in this privacy notice, please contact our **Data Protection Officer**:

- Gary Botha, Business Manager
- 01753 598300
- garybotha@lgs.slough.sch.uk

Appendix 3 – Personal data breach procedure

Definition

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

Reporting breaches

All staff are required to report data breaches or potential data breaches. Staff should adhere to the precautionary principle – that is, even if staff are unsure whether or not a breach of personal data has taken place they should still report it.

If a breach or potential data breach is revealed, it must be reported as soon as possible to the DPO, Gary Botha. The report can be made in person or by email marked high priority

If a member of staff reports a breach by email but does not receive acknowledgement within 24 hours then **he or she must follow this up** by reporting the incident to another member of the school's Senior Leadership Team (SLT) ideally in person, or failing that on the phone, or failing that, by emailing everyone on the SLT marking the email as 'high priority'.

These procedures apply throughout the year, even at weekends or during school holidays.

Staff should be aware that the school, along with all organisations, has a legal duty to report breaches of personal data to the Information Commissioner's Office within 72 hours of them occurring. This requirement came into force in May 2018 under the GDPR.

Responding to the report of a breach in personal data

On receiving a report of a data breach, the DPO, or another senior member of staff acting on behalf of 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

If it is likely that a breach of personal data has taken place the DPO will alert the headteacher

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. Examples of actions relevant to specific data types are stated below:

- If the network credentials of a colleague, student or governor has been compromised, the user will be asked to immediately change his or her password and the ICT manager will be asked to investigate any unauthorised access.

- 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
    - If the sender is unavailable or cannot recall the email for any reason, the DPO will ask the ICT department to recall it
    - In any cases where the recall is unsuccessful, the relevant unauthorised individuals who received the email may be contacted to 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 and seek a written request that this request has been complied with.

Meanwhile 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) along with details of the breach, in case it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions will be stored on the school's GDPRiS portal.

Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website within 72 hours. As required, the DPO will set out:

- A description of the nature of the personal data breach including, where possible:
    - The categories and approximate number of individuals concerned
    - The categories and approximate number of personal data records concerned
- The name and contact details of the DPO
- A description of the likely consequences of the personal data breach
- A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned

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

The DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPO will promptly inform, in writing, all individuals whose personal data has been breached where this is known. 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

Actions to mitigate against future breaches of personal data

Following a data breach, the DPO will put in place measures, as appropriate, to reduce the likelihood of a similar breach in future. Actions taken may include but are not limited to, more robust processes for storing data, disposing of data or providing further training for individuals.

Appendix 4 – Key expectations for staff

As a school we expect all staff to take the protection of personal data seriously. In order to reduce the risk of a potential data breach and to mitigate the impact of a data breach, should it occur, we have the following key expectations of staff. These expectations are not exhaustive, they should be read alongside our data protection policy.

Data storage

- Papers containing *sensitive* personal data (for example, counselling records, SEN and health information, parents' personal contact details) must be kept securely (for example in a locked cupboard, desk, office or filing cabinet).
- Papers containing *less sensitive* personal data (for example, students' assessment results) should not be left on display: they should not be left lying around on teachers' desks in classrooms, pinned to notice/display boards, nor left anywhere else where there is general access. Such information should be filed away out of sight.
- Unencrypted memory sticks (flash drives), external hard drives or similar must never be used to store personal data, and the use of memory sticks generally is discouraged.
- Reasonable steps should be taken to ensure that portable devices (for example laptops, iPads) containing personal data are kept securely when taken out of school (for example, not in view in a parked car).

Disposal of documents containing personal data

- Paper documents containing personal data, sensitive or otherwise, (e.g. medical information, contact details (other than school email addresses), students' assessment results, SEN information) must be shredded, rather than placed in recycling or waste paper bins.

Password security

- Passwords that enable access to websites or systems containing personal data (for example Office 365, the school network, SIMS) must not be written down or disclosed (except where necessary for initially setting up ICT accounts).
- Passwords that enable access to personal data, should, where possible, be sufficiently complex so they cannot be guessed easily and can resist 'brute force' attacks i.e. ideally be at least 8 characters long and include a mix of capital and lowercase letters, numbers and symbols.
- Passwords that enable access to websites or systems containing personal data should be changed at regular intervals (i.e. termly).

Sharing personal data with third parties

- Staff must contact the DPO (Gary Botha) or the Data Manager (Rowena Gaiger) for advice on procedures before sharing personal information with third parties (i.e. people beyond the school or other organisations)

Reporting data breaches

The school has a legal duty to report breaches of personal data that meet certain thresholds to the ICO within 72 hours. **All staff are therefore required to report data breaches or potential data breaches.** These procedures apply throughout the year, even at weekends or during school holidays. Staff should adhere to the precautionary principle – that is, even if staff are unsure whether or not a breach of personal data has taken place they should still report it.

If a breach or potential data breach is suspected or revealed, it must be reported as soon as possible to the DPO, Gary Botha. The report can be made in person or by email marked high priority.

If a member of staff reports a breach by email but does not receive acknowledgement within 24 hours then **he or she must follow this up** by reporting the incident to another member of the school's Senior Leadership Team (SLT) ideally in person, or failing that on the phone, or failing that, by emailing everyone on the SLT marking the email as 'high priority'.

Staff should be aware that the school, along with all organisations, has a legal duty to report breaches of personal data to the Information Commissioner's Office within 72 hours of them occurring.