THE GRAMMAR SCHOOL AT LEEDS
Be Inspired

DATA PROTECTION POLICY

ISI Reference:	
Rationale for the Policy:	This policy is created to ensure that The Grammar School at Leeds, GSAL Transport Ltd, and GSAL Enterprises (together GSAL) meets its data protection obligations, including those provided for in data protection legislation, whilst adhering to statutory requirements already extant within the education sector.
Policy aim:	To provide guidance for staff, parents and the wider community in fulfilling data protection requirements.

Author:	Graham Purves
Agreed and Authorised by:	GSAL SLT
Date agreed:	August 2023
To be reviewed:	November 2026

Date of review:	August 2023
Dates of interim amendments/updates:	

Category:	Internal/External
Circulation and publication:	All staff

The School runs on FREDIE principles:
Fairness, Respect, Equity, Diversity, Inclusion and Engagement

1. Introduction

This policy sets out the school's commitment to data protection and individual rights and obligations in relation to personal data. As part of its normal day-to-day operations, the school holds and processes personal data regarding prospective, current, and former: employees, parents, students, alumni, students applying for admission and their parents, suppliers, visitors, agents, and friends.

The principles of GDPR shall be applied to all data processed by the school. GSAL commits to:

- Ensure that data is processed fairly, lawfully and transparently;
- Process data only for defined specific, explicit and legitimate purposes;
- Ensure that all data processed is adequate, relevant and not excessive;
- Ensure that data processed is maintained accurate and up to date where necessary;
- Not keep data longer than is necessary of the purposes for which it was collected;
- Ensure that data is processed securely.

In addition, GSAL and the individuals within it take responsibility for what we do with personal data and how we comply with the principles outlined above. This is known as the Accountability Principle.

The school regularly reviews all manual and electronic files to ensure compliance with these principles; to ensure security and integrity of filing systems and to ensure that access to them is only available to an authorised person(s).

Related and connected laws;

- The Data Protection Act 2018
- The UK General Data Protection Regulation
- The Common Law Duty of Confidentiality
- Privacy and Electronic Communications Regulations 2003
- Computer Misuse Act 1990
- Human Rights Act 1998

2. General principles and scope

2.1. The Grammar School at Leeds is committed to the protection of all personal and special categories of personal data for which it holds responsibility as the Data Controller, and the handling of such data in line with data protection principles and data protection law (together "General Data Protection Regulation and Data Protection Act 2018"). Any changes to Data Protection Laws will be monitored and implemented where necessary to remain compliant with these requirements. Employees of the school will receive regular notifications and adequate data protection training to maintain so as to ensure on-going awareness of and compliance with these requirements.

2.2. GSAL shall maintain a framework of policies and procedure documents setting out the organisation's approach to data protection matters and the control measures in place to ensure compliance with and accountability to data protection matters. GSAL will ensure that these documents are reviewed periodically to:

a) test their adequacy in meeting the legal standards as they change over time; and

b) to test the school's compliance with them.

2.3 GSAL shall ensure that all relevant personnel and/or other persons its commissions to process personal data on its behalf, either directly or indirectly, have received appropriate and sufficient training in the application of the organisation's policies.

2.4 In accordance with regulatory requirements, the school has notified the Information Commissioner's Office of its processing activities. The school's ICO registration number is Z6909893 and its registered address is: The Grammar School at Leeds, Harrogate Road, Leeds,

LS17 8GS.

2.5 The requirements of this policy are mandatory for all staff, volunteers and casual or supply workers employed by the school and any third party contracted to provide services within the school. This policy applies to all activities or operations which involve the processing of personal data.

3. Terms and abbreviations

- **GDPR – The UK General Data Protection Regulation 2021** GDPR is UK Law that is designed to harmonise data protection laws and guarantee the rights and freedoms of individuals;
- **ICO – Information Commissioner's Office**. The Information Commissioner is an independent official appointed by the Crown. The Commissioner's decisions are subject to the supervision of the Courts and the Information Tribunal. The Office's mission is to "uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals.";
- **Personal Data** – means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;
- **Special Categories of Personal Data –** means any personal data relating to race, ethnic origin, political opinions, religion, philosophical beliefs, trade union membership, genetic data, biometric data, health data, data concerning a natural person's sex life, sexual orientation, safeguarding concerns, pupils in receipt of pupil premium, pupils with special educational needs and disability (SEND), children in need (CIN), children looked after by a local authority (CLA).
- **Criminal offence data** is personal data that is treated in a similarly sensitive way to special category data. It records criminal convictions and offences or related security measures. Criminal offence data includes: the alleged committing of an offence, the legal proceedings for an offence that was committed or alleged to have been committed, including sentencing. Schools process criminal offence data in storing the outcome of a Disclosure and Barring Service (DBS) check on their employees, non-employed staff and volunteers. As these data relate to criminal convictions, collecting and retaining it means the school is processing criminal offence data. This applies even though the check has not revealed any conviction. You can read about handling DBS data in the statutory guidance on keeping children safe in education.

- **DSAR – Data Subject Access Request** is the process by which an individual (data subject) can request access to data about them held by the school (*see section 7*);
- **Data Controller** - means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;
- **Data Processor** - means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;
- **Data subject** - any living individual who is the subject of personal data held by an organisation. A school's data subjects include:
    - pupils and former pupils
    - parents and carers
    - employees and non-employed staff
    - governors and trustees
    - local-authority personnel
    - volunteers, visitors and applicants
- **Information Asset Owner** - the person responsible for the instigation or on-going maintenance of a data process or data processing operation;
- **Identifiable living individual** - means a living individual who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data or an online identifier, or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the individual;
- **Processing** - means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;
- **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 transmitted, stored or otherwise processed; data breaches can be deliberate or accidental
- **Risk** - the chance of something happening, which will have an impact upon objectives. It is measured in terms of consequence and likelihood;
- **Risk Management** - the culture, processes and structures that are directed towards the effective management of potential opportunities and adverse effects;

- **Recipient** - means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing;
- **Third party** - means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data;
- **Profiling** - is any form of automated processing of personal data intended to evaluate certain personal aspects relating to a natural person, or to analyse or predict that person's performance at work, economic situation, location, health, personal preferences, reliability, or behaviour. This definition is linked to the right of the data subject to object to profiling and a right to be informed about the existence of profiling, of measures based on profiling and the envisaged effects of profiling on the individual;
- **Consent** - means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data;
- **'The school' –** refers to The Grammar School at Leeds unless otherwise stated.

4. Responsibilities

Data Controller
The School is the legal data controller under Data Protection Legislation for the data it collects and processes.

Management and supervisory staff
The board of governors are accountable for the management of the school and ensuring appropriate technical and organisational measures are in place to ensure an appropriate level of data protection is maintained and mechanisms are in place to support service delivery and continuity. Maintaining confidentiality is pivotal to the school being able to operate.

Each board member in their respective areas of responsibility, must ensure that all staff members are aware of this policy, other relevant policies and procedures, and of their responsibilities concerning the processing of personal data. They are responsible for ensuring that anyone processing data is sufficiently aware of this policy, how it applies to their job role and sufficiently trained to carry out their duties in compliance with this policy.

Data Protection Lead
The Data Protection Lead is responsible for providing the policies, guidance and training needed to ensure the school is compliant with Data Protection Laws and privacy risks are assessed accordingly. They will monitor and report to the governing body in respect of compliance with this policy, investigate any breaches, and maintain suitable records of processing activities. They may co-opt other individuals to assist with the management of data protection obligations. The Data Protection Lead is responsible for monitoring Data Protection legislation, case law, guidance, and codes of practice and incorporating relevant changes into the school's policy.

Employees, volunteers, casual/temporary workers etc.
Anyone who is directly engaged by the school to undertake data processing activities (including but not limited to employees, volunteers, casual/temporary workers etc.) involved in the receipt, handling or communication of personal data must adhere to this policy. Anyone who is not confident in or has concerns about handling practices that they are undertaking, or witnessing should contact the Data Protection lead. Individuals are expected to complete appropriate mandatory training. Everyone within the School has a duty to respect data subjects' rights to confidentiality.

Partner & third-party responsibilities
Any third party or organisation that is commissioned to process data or receives data from the school or is able to access any personal data must enter into a legally enforceable agreement that satisfies the requirements of the GDPR. Any such agreement must be approved by the Data Protection Lead.

5. Policy detail

5.1. Fair lawful and transparent processing
The processing of all personal data by the school must be undertaken in a fair, lawful and transparent manner, this means:

Fair – no data collection activities to be undertaken or commissioned without an appropriate privacy notice being provided to the person from whom data are being collected and to the people who the data are about if personal data are collected from sources other than the data subject. All privacy information and any changes to privacy information must be approved by the DPL.

Transparent – the data subject must be informed of the reasons why personal information is collected, what it will be used for, whom it will shared with, how long the information shall be retained for, what the lawful basis for processing is, what their rights are and how to enforce these in a clear, transparent and easily understood privacy notice.

Lawful – no data collection activities are to be undertaken or commissioned without there being a lawful basis for the data processing activities. The DPL is responsible for assisting staff with determining the lawful grounds for processing. Where the lawful ground requires the data subject's consent, consent must meet the conditions for consent as defined by the GDPR to be valid. Where consent is relied upon this must be documented to demonstrate the validity of consent and to address the principle of accountability.

Where the lawful basis for processing relates to a legitimate interest, a legitimate interest assessment (LIA) shall be undertaken, documented and retained by the DPL. Each information asset owner is responsible for ensuring that there are lawful grounds for all data processing activities that fall under their responsibility and LIAs are properly undertaken where necessary. The DPL will provide advice regarding lawful processing conditions. A *legitimate interest assessment template* can be found on GSAL World / Staff / All Staff / Data Protection and GDPR / Forms and Templates.

The school publishes privacy information on its website as a primary means of communication and also at various points where personal data is collected. The school ensures that appropriate privacy information is made available to data subjects at the point of data capture. The school undertakes the processing of personal data for a variety of purposes and on a range of lawful bases and will ensure that these are provided to data subjects via privacy information. Privacy information including statements of consent designed for children (aged 13 or under) will be written using clear and age-appropriate language.

5.2. Data processing purposes

Personal data is only to be collected, created or otherwise obtained for specific, explicit and legitimate purposes. No data processing is to be undertaken or commissioned without the approval of the DPL who shall maintain a register of data processing activities (via the Information Asset Register). Data process owners are responsible for ensuring that all of the data processing activities that they undertake and/or commission have been approved by the DPL. No personal data shall be used for any purpose other than that for which it was collected and/or created for without the approval of the DPL or a senior member of the management team.

5.3. Data minimisation

The school strives to use a minimum of personal data in its data processing activities and periodically reviews the relevance of the information that it collects. Data process owners are responsible for ensuring that no unnecessary, irrelevant or unjustifiable personal data are collected or created either directly or indirectly through the data processing activities they are responsible for and/or engage in. The DPL will provide advice regarding the justification of personal data collected or created.

5.4. Data accuracy

We recognise that the accuracy of data is important and that some data are more important to keep up-to-date than others. The school will ensure to maintain data as accurate and up-to-date as possible, in particular data which would have a detrimental impact on data subjects if it were inaccurate or out-of-date For example, contact information of a parent in an emergency. Information Asset Owners are responsible for ensuring that personal data they have collected or created either directly or indirectly through the data processing activities they are responsible for and/or engage in are maintained as accurate and up-to-date. Personal data whose accuracy cannot reasonably be assumed to be accurate and up-to-date are treated appropriately through correction, erasure or anonymisation measures. The DPL will provide advice regarding data accuracy.

5.5. Data retention

The school does not retain personal data for any longer than is necessary for the purposes for which they were collected and applies appropriate measures at the end of data's useful life such as erasure or anonymisation. Data process owners are responsible for determining the retention period for personal data under their control. The DPL must approve all retention periods for personal data and ensure that this is correctly logged on the retention schedule. The accurate retention of data is a vitally important issue, as both the over-retention and under-retention of personal data could have a

detrimental impact on both the data subject and the organisation. The DPL will undertake regular data retention audits to ensure compliance with stipulated retention periods.

The DPL can provide detailed guidance to staff on the statutory and/or recommended retention periods for the core processing activities and for different types of personal data. However, it is recognised that not every eventuality can be outlined in such a policy, and staff are expected to use their professional judgement on whether data they hold on personal drives and within emails (other than in cases with statutory retention periods) remains necessary to the running of the school or their role within the school.

Paper-based personal data which needs to be disposed of should be placed in one of the secure, locked bins provided in locations throughout the school. All materials placed in these containers is securely destroyed by shredding. The school limits access to its confidential waste awaiting destruction.

Electronic personal data that is no longer needed should be deleted from all local, cloud based or online storage locations. Staff are expected to 'double delete' all such records to ensure that they are fully removed from devices and all storage locations. Emails containing personal data should similarly be 'double deleted' when they are no longer needed.

For further information please refer to the schools *Retention Schedule* which can be obtained on GSAL World / Staff / All Staff / Whole School Policies / GDPR.

5.6. Information security

Any personal data that the school processes or commissions the processing of is processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures. In particular the Information Security Management Policy (ISMP) sets out specific policies in relation to maintaining the security of personal data. The DPL is responsible for the formulation of the ISMP.

All staff members are responsible for ensuring that they take reasonable appropriate measures to protect personal data and prevent its loss and unauthorised or unnecessary destruction, disclosure or dissemination. This means that staff must ensure that any personal data they hold is kept securely, and that it is not disclosed either orally or in writing or otherwise to any unauthorised third party without there being a lawful basis for the disclosure and without prior approval from the DPL.

Paper-based records and portable electronic devices, such as laptops and hard drives which contain personal data are kept under lock and key when not in use. The creation of unnecessary paper copies of personal data is to be avoided. Papers containing confidential personal information should not be left on office or classroom desks, on staffroom tables or pinned to noticeboards where there is general access. This is contrary to the clear desk policy and security principles relating to the safe handling of personal information.

Where personal information needs to be taken off site (in paper or electronic form) staff are responsible for ensuring that suitable steps are taken to ensure that it is kept safe and secure, and not accessible to anybody who is not authorised or entitled to have access to it.

The school's Acceptable Use Policy sets out the terms on which staff and students may use the school's data systems, infrastructure, and where required for their role personal data. All staff and students are required to signify that they accept and will abide by the Acceptable Use Policy.

Staff are responsible for ensuring that all portable devices and removable media they use to process, store or transport personal data (such as laptops, phones, home computers and USB devices) are suitably protected via passwords and/or encryption software. Staff, pupils or governors who store

personal data on their personal devices are expected to follow the same security procedures as for school owned devices. For example, all personal devices are required to have appropriate security controls in place. e.g. passcode.

5.7. Record keeping and accountability

In order to fulfil its responsibility to be able to demonstrate compliance with data protection legislation as well as in support the policy on transparency the school maintains records of the processing activities that it controls, undertakes or otherwise commissions as required by the data protection legislation and specifically those required in Article 30 of the GDPR. This will be in the form of the Information Asset Register.

5.8. Information rights

The school recognises the legal rights of those whose data it is processing or intends to process including:

- Right to information about data processing operations
- Right of access to personal data
- Right to portability of personal data
- Right of rectification of personal data
- Right of erasure of personal data
- Right to restriction of processing
- Right to object to direct marketing
- Right to object to data processing operations under some circumstances
- Right not to be subject to decisions made by automated processing under some circumstances
- Right of complaint about the organisation's processing of personal data and the right to a judicial remedy and compensation

The School will process Data Subject Rights within one calendar month of receiving a request at no cost to the data subject.

The school publishes appropriate information within its privacy notice to advise data subjects of their rights. Policies and procedures are produced to guide and support all staff in recognising an information rights requests and how to handle them appropriately when they are exercised. The school provides training where necessary to those staff who may need assistance in the handling of data subject rights requests. For further information including exemptions, please refer to the schools *Procedure for Handling Information Rights Requests* (GSAL World / Staff / All Staff / Data Protection / Documentation / Procedures and Guidance)

All rights requests are to be raised via email to dpo@wntai.co.uk

5.9. Consent

The school interprets consent to be as defined in the GDPR and that any consent shall not be valid unless:

- there is a genuine choice;
- it has been explicitly and freely given, and represents a specific, informed and unambiguous indication of the data subject's wishes that signifies agreement to the processing of personal data relating to them;
- the consent was given through statement made by the data subject or by a clear affirmative action undertaken by them;

- the school can demonstrate that the data subject has been fully informed about the data processing to which they have consented and is able to prove that it has obtained valid consent lawfully;
- a mechanism is provided to data subjects to enable them to withdraw consent and which

makes the withdrawal of consent in effect as easy as it was to give and that the data subject has been informed about how to exercise their right to withdraw consent.

The school recognises that consent may be rendered invalid in the event that any of the above points cannot be verified or if there is an imbalance of power between the data controller and the data subject. The organisation recognises that consent cannot be considered to be forever and will determine a consent refresh period for every instance where consent is the lawful condition for processing.

5.10. Personal data breaches

The school maintains a procedure for handling security incidents and personal data breaches and ensures that all employees and those with access to personal data are aware of their responsibilities when discovering a breach.

Let a member of ELT know at the first opportunity, making a record of: what was shared; how it was shared; who it was shared with. In addition employees and individuals should report all personal data breaches using the personal data breach reporting form on GSAL World (GSAL World / Staff / All Staff / Data Protection / Report a GDPR breach) and adhere to the guidance set out in the *Procedure for Handling Security Incidents and Personal Data Breaches* as soon as they become aware of an actual or potential breach.

The school will log all personal data breaches and will investigate each incident immediately. Appropriate remedial action will be taken as soon as possible to isolate and contain the breach, evaluate and minimise its impact, and to recover from the effects of the breach. Data protection near misses will also be recorded and investigated in the same manner as data protection breaches. The breach reporting procedure will set out responsibilities, decision-making criteria and timescales for notifying data subjects, the Information Commissioner and the media about a personal data breach. Where a breach is notifiable to the Information Commissioner this must be made within 72 hours of becoming aware of the data breach occurring.

For further information please refer to the *Procedure for Handling Security Incidents and Personal Data Breaches* (GSAL World / Staff / All Staff / Data Protection / Documentation / Procedures and Guidance).

5.11. Data protection non-compliances

The school takes seriously any potential breaches of its duty to process personal data in accordance with data protection law. If a data subject believes that the school has not complied with any of its data protection policies or procedures or acted otherwise than in accordance with the General Data Protection Regulation, they should in the first instance inform the school's Data Protection Lead in writing, either by letter or email. The Data Protection Lead will always investigate possible data breaches and non-compliances and maintain a record of such complaints to allow it to reflect upon and develop its practice, policies, training or staff awareness.

5.12. Data processors

The school reserves the right to contract out data processing activities or operations involving the processing of personal data in the interests of business efficiency and effectiveness. No third party data processors will be appointed without being subject to appropriate risk assessments in line with applicable Data Protection Legislation.

Individuals wishing to appoint a data processor must ensure that appropriate due diligence is undertaken on the proposed data processor in the field of information governance and data protection compliance prior to their appointment. The DPL will provide advice and guidance in respect of this. A written agreement will be implemented between the school and the data processor which meets the requirements of the Data Protection Legislation. The DPL will ensure that a register of such agreements/arrangements is maintained. The data processor agreement will specify what is to happen to personal data upon termination of the data processing agreement.

No employee is permitted to commission or appoint a third party to process data on behalf of the organisation without adhering to this policy.

For further information and guidance, please refer to the *Procedure for Managing Data Processors, Disclosures and Data Sharing* (GSAL World / Staff / All Staff / Data Protection / Documentation / Procedures and Guidance).

5.13. Data sharing, disclosure and transfer

The school has a number of contracts with third party organisations which assist with the delivery of educational, employment and other functions and pursuant to the fulfilment of contractual obligations and/or business efficiency and effectiveness. Additionally, the school is sometimes required by law or in the best interests of the students or staff to disclose personal data with external authorities (such as the local authority, health and social services, police, Independent schools' Inspectorate, or the Department for Education).

The School shall ensure the following:

- Prior to disclosing any personal data to third parties the school may undertake a risk assessment relating to the disclosure.
- The school will only share personal data with or otherwise disclose personal data to other organisations and third parties where there is a legal basis for doing so and where the data sharing is necessary for specified purposes.
- No data sharing or disclosure is permitted to occur without a suitable legally enforceable agreement satisfying the requirements for such agreements as set out in the Data Protection Legislation being in place.

When the school discloses personal data with a third-party organisation, only the personal data necessary for the purpose (e.g. the completion of a contract, legal obligation, of the undertaking of the legitimate interest) is provided by the school.

Where formal agreements cannot be obtained from third party organisations seeking data held by the school, then consent to share data will be obtained in advance from the data subject. One (but not the only) example of this includes student university applications for countries outside of the UK.

For further information and guidance, please refer to the *Procedure for Managing Data Processors, Disclosures and Data Sharing* (GSAL World / Staff / All Staff / Data Protection / Documentation / Procedures and Guidance).

5.14. Data transfers

The school provides information to all staff setting out safe and approved methods of transferring personal data to recipients. Employees are required to use only approved methods of data transfers. Disciplinary action will be taken against employees who fail to observe the data transfer policy and use unsafe and insecure methods of data transfer unless such methods have been approved in writing by the DPL.

5.15. International transfers of personal data

The school neither transfers nor process nor will it permit personal data to be transferred or processed outside the UK without the conditions laid down in the Data Protection Legislation being met to ensure that the level of protection of personal data are not undermined. Any transfer or processing of personal data that the organisation undertakes or commissions whether directly or indirectly must be approved by the DPL and may only take place if one of the following is satisfied:

- The territory into which the data are being transferred is one approved by the UK's Information Commissioner;
- The territory into which the data are being transferred has an adequacy decision issued by the UK Government;

- The transfer is made under the unaltered terms of the standard contractual clauses issued by the Information Commissioner's Office for such purposes;
- The transfer is made under the provision of binding corporate rules which have been approved and certified by the UK Government;
- The transfer is made in accordance with one of the exceptions set out in the Data Protection Legislation.

Transfers of personal data overseas will be recorded on the records of processing activities and privacy information as necessary.

5.16. Risk assessment

The school embraces the principles of privacy by design and by default. Data protection impact assessments (DPIA) are to be undertaken and documented where the DPIA screening questionnaire indicates the requirement. Appropriate resources are made available to advise on DPIAs where this should be sought. The DPL is responsible for maintaining a Data Protection Risk Register of compliance risks that have been identified by the organisation.

For further information, please refer to the *Procedure for Data Processing Risk Assessments* which can be found in GSAL World / Staff / All Staff / Data Protection / Documentation / Procedures and Guidance).

5.17. Children's data

Special measures are be taken by the school when it processes personal data relating to children under the age of 13, including the nature of privacy information provided and approach to information rights requests and ensuring that these are clear, transparent, age relevant and understandable.

Employees must make every reasonable effort to ensure that any pupil under the age of 13 whose parent has refused permission for information about their child, including images, to be used for publicity purposes are not used for such activities. Where pupils are over the age of 13 permission can be refused by the pupil themselves.

Employees must also ensure that any use of 'special category' personal data for publicity purposes has specific and explicit consent from the parent and/or pupil, if competent, to do so.

5.18. Taking, storing and using images of children

The school provides guidance to staff on taking, storing and using images of children and on the importance of ensuring that images of children are made and used responsibly, only for school purposes, and in accordance with school policies and the law.

For more information please refer to the Taking, Storing and Using Images of Children Policy (GSAL World / Staff / All Staff / Whole School Policies / GDPR)

5.19. Training and awareness

The school requires all those who it engages to process personal data either directly or indirectly are provided with appropriate training in the application of this and other data protection policies and procedures and in their data protection responsibilities. It will also undertake data protection awareness raising activities from time to time to keep data protection front of mind. All training and awareness raising activities will be logged. Refresher training will be provided annually.

5.20. Audit and compliance checking

The school undertakes periodic compliance checks to test whether its policies and procedures are being adhered to and to test the effectiveness of its control measures. Corrective action is taken where no-conformance is found. Records are kept of all such audits and compliance checks including corrective action requests raised. Disciplinary action will be taken against individuals who fail to act upon the reasonable corrective action. The governing body Audit and Risk Committee will be provided with a summary of audit findings on a termly basis.

6. Related policies and documents

- Data Retention Policy
- Privacy Notices
- Password Policy
- Staff Acceptable Use Policy
- Pupil Acceptable Use Policy
- Staff Code of Conduct

Further information about GDPR and Data Protection can be obtained via:

GSAL Data Protection Lead
Data Protection Officer
The Grammar School at Leeds
Alwoodley Gates
Harrogate Road
Leeds
LS17 8GS
dpo@wntai.co.uk

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF
https://ico.org.uk/

Appendix A - Steps you must take to protect data

November 2022

This is a critically important part of our work in school and all colleagues must follow the following basic rules

1. Telephone calls

Who are you speaking to? – how do you know who you are speaking to?
Follow the identity verification procedure:

- Police or other officials – ask for identification number, and then call them back on a publicly available number for their organisation.
- Parent – check that they are listed as a contact on SIMS. If they are not, end the call and inform the DSL immediately. If they are, ask a security question to validate (their child's middle name, their contact email address – something you can see on the child's home page on SIMS as you speak).

Full details can be found in appendix A.

2. E-mail with personal or school data/information

Before you send an email with any personal information or school information, ask yourself the following questions.

- Do you have a right to share the data?
- Do they have a right to access the data?
- Instead of sending an attachment, can you tell them to where to find it, (on SharePoint, GSALWorld, etc)?
- Am I sharing only what is necessary?
- Am I sharing only with people who need it?

Sharing with GSAL staff

- Send links to OneDrive or SharePoint files, instead of sending attachments. Only send an attachment, if there is no alternative, and if there are any sensitive data, password protect the attachment.
- If you send a password, send it through a separate system, eg Teams Chat, or pass it directly to the person.

Sharing outside GSAL

- Verify who you are sending it to.
- Password protect any personal information if sending to a third party (ie if sending something about a child to their parents you don't need to password protect, if sending something about a child to a professional outside GSAL you should password protect it)
- Share the password separately

Sharing with GSAL pupils

- Do not share one pupil's personal information with another pupil.
- Only share information with a pupil that is in a form we would want them to see.

Before you send

THINK

have you followed all of the steps?
if you have any doubts, check with your line manager.

For support:

check with your line manager;
speak with a member of the PA team, they can support with the necessary steps and advice.

If you share data in error

Let a member of ELT know at the first opportunity making a record of: what was shared; how it was shared; who it was shared with.

Appendix B – Identity verification

Purpose

Under the General Data Protection Regulation (GDPR), GSAL is obliged to take reasonable steps to confirm the identity of anyone requesting personal data. GSAL also has an obligation to its pupils, parents and staff to ensure their personal data are handled properly.

This procedure sets out the steps that must be taken prior to the disclosure/sharing of personal data.

Where the request is from a third party, employees must follow the Procedure for managing data disclosures (GSAL World / Staff / All Staff / Data Protection and GDPR / Procedures and Guidance) before sharing or disclosing any information.

Roles and responsibilities

Support staff employees are prohibited from disclosing or sharing personal data unless this procedure is followed due to the great number of interactions with many different people and the potential risk of misidentifying them.

Teaching employees are encouraged to follow this procedure where they feel it is necessary.

Procedure

1. Identity verification of the police

Employees must ask to see the police officer's official ID if physically present, or, if the contact is by phone, record the police officer's identification number and ask for the police officer's station and name of senior officer. Employees should call the senior officer using a publicly available phone number to confirm the officer's identity.

2. Identity verification of a caller

2.1. From the individual themselves or by a parent/guardian/close contact

If the caller claims to be a parent or other close contact of a pupil, employees should check whether the caller is listed as a contact against the child in SIMS. If the caller is not listed, politely end the call and notify the Designated Safeguarding Lead and Data Protection Lead immediately. If the caller is listed as a contact continue to follow the steps below.

The best way to verify identity over the phone is by asking some security questions. Security questions build trust, as individuals are reassured that suitable precautions are being taken. Employees should always ask a minimum of two questions (e.g. one about the parent and one about the pupil), and three questions if you are being asked to disclose sensitive information such as financial or medical information.

Security questions should avoid information that can easily fall into the wrong hands. Household bills are often thrown out intact, handbags are stolen, cars broken into, and documents lying around can fall into the wrong hands. Some answers are easily guessed if a caller has even a tiny bit of
information about the individual. The trick is to find the balance between something that a genuine caller can answer and something that doesn't appear on many documents.

Examples of security questions include:

· What is your email address (home/work)?
· What is your phone number (mobile/home/work)?
· What method do you use to pay school fees?
· What is your child's admission number?
· Who is your child's form tutor/class teacher?
· What is your middle name/your child's middle name?
· What month and year did you commence employment at GSAL? (for staff)

Do not be afraid to politely refuse the request of a caller that cannot give the correct answers.

2.2. From a third party, e.g. another school or agency including children social work services

For routine requests employees should ask the caller to email the request. From this email you can verify the email address that it has been sent from and keep a record of who has asked for information. Once the email request is received see below section 3. Information requested by email.

If the matter is time critical or it would be more beneficial to have a telephone conversation with the caller, for example regarding a safeguarding concern, employees have the option of taking the caller's name and organisation and calling them back on a publicly available telephone number.

In this case do not use a number given to you by the caller, employees must visit the organisation's website and call the main contact number listed.

3. Identity verification of an email sender

The identity of a person requesting information via email can be verified by checking their email address or email domain (e.g. @gsal.org.uk).

3.1. Emails from a person known to GSAL

· Has the email been sent from an email address that is recorded in a school database?

If the email address is different to that recorded in a GSAL database, employees should ask the sender to send the email from a recognised email account. If they no longer use the account on record, employees should ask them to confirm their identity by asking a minimum of two security questions as listed in section 2.1 of this procedure.

3.2. Emails from an organisation

· Is this the same email domain as listed on their website?

If the email domain is different to that on the organisation's website do not disclose any information. For example, the email address is XXX@abc.com but their website states email addresses follow the format XXX@abc.co.uk.