Godstone Primary and Nursery School



Data Protection and GDPR Policy

REVIEW DATE: September 2026
REVIEWED BY: Governing Body
NEXT REVIEW: September 2027
WRITTEN BY: Nick Usher

Headteacher: Nick Usher
Chair of Governors: Liam McGivern

1. Aims

Godstone Primary and Nursery School is committed to protecting the privacy and security of personal data relating to pupils, parents and carers, staff, governors, volunteers, visitors and other individuals whose information the school processes. The school will comply with all applicable data protection legislation and will ensure that personal data is:

- processed lawfully, fairly and transparently;
- collected for specified, explicit and legitimate purposes;
- adequate, relevant and limited to what is necessary;
- accurate and, where necessary, kept up to date;
- retained only for as long as necessary;
- processed securely and protected against unauthorised or unlawful processing, loss, destruction or damage; and
- managed in a way that enables the school to demonstrate its compliance.

Data protection is the responsibility of everyone working within or on behalf of the school. All staff, governors, volunteers and contractors must understand their responsibilities when handling personal data.

This policy applies to personal data in all forms, including paper records, electronic records, photographs, video, audio recordings, CCTV, biometric information and information stored or processed through online systems and educational technology.

The school will also take account of the specific requirements that apply when processing children's personal data and will place particular emphasis on children's privacy, safety and rights.

2. Legislation and guidance

This policy has regard to the following legislation and guidance:

- UK General Data Protection Regulation (UK GDPR), as amended;
- Data Protection Act 2018;
- Data (Use and Access) Act 2025;
- Privacy and Electronic Communications Regulations 2003, where applicable;
- Education (Pupil Information) (England) Regulations 2005;
- Freedom of Information Act 2000;
- Protection of Freedoms Act 2012, in relation to biometric information;
- relevant statutory safeguarding guidance, including Keeping Children Safe in Education;
- Department for Education guidance on data protection in schools;
- Information Commissioner's Office (ICO) guidance and codes of practice; and
- other relevant legislation and regulatory requirements applicable to the school.

The Data (Use and Access) Act 2025 amended aspects of UK data protection law and its data protection provisions are now in force. The school will review its procedures as further regulatory guidance is issued.

3. Definitions

Term	Definition
Personal data	Information relating to an identified or identifiable living individual. This can include names, identification numbers, contact details, location information, online identifiers, photographs, recordings and information about an individual's physical, physiological, genetic, mental, economic, cultural or social identity.
Special category data	More sensitive personal data requiring additional protection. This includes information about racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data used for identification, health, sex life and sexual orientation.
Processing	Anything done with personal data, including collecting, recording, storing, organising, retrieving, using, sharing, altering, restricting, deleting or destroying it.
Data subject	The identified or identifiable individual to whom personal data relates.
Data controller	The organisation that determines the purposes and means of processing personal data.
Data processor	An organisation or individual that processes personal data on behalf of the data controller.
Personal data breach	A breach of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.
Consent	A freely given, specific, informed and unambiguous indication of an individual's wishes by which they signify agreement to the processing of personal data.
Data Protection Impact Assessment (DPIA)	A process used to identify and minimise data protection risks arising from processing activities that are likely to result in a high risk to individuals.
Privacy notice	Information provided to individuals explaining how and why the school collects, uses, stores and shares their personal data.

4. The data controller

Godstone Primary and Nursery School is the data controller for the majority of personal data it processes. As data controller, the school is responsible for determining:

- what personal information it collects;
- why it collects and uses that information;
- how information is processed;
- who information may be shared with;
- how long information is retained; and
- how individuals' data protection rights are supported.

The school is registered with the Information Commissioner's Office (ICO) and will maintain its registration and pay any applicable data protection fee.

Where the school processes personal data jointly with another organisation, or where another organisation determines the purposes and means of processing, the respective responsibilities will be established and documented.

5. Roles and responsibilities

This policy applies to all staff employed by the school and to governors, volunteers, contractors, agency workers, external organisations and individuals processing personal data on behalf of the school. Failure by a member of staff to comply with this policy may result in disciplinary action.

5.1 Governing Body

The Governing Body has overall responsibility for ensuring that the school complies with its data protection obligations. The Governing Body will:

- ensure appropriate data protection policies and procedures are in place;
- ensure the school has appropriate resources to meet its data protection responsibilities;
- support the work of the DPO;
- receive appropriate reports and assurance regarding data protection compliance;
- ensure significant risks are appropriately managed; and
- ensure the policy is reviewed regularly.

5.2 Data Protection Officer

The school's Data Protection Officer (DPO) is provided by Judicium Education**.** The DPO is responsible for advising and supporting the school in relation to data protection compliance and for monitoring compliance with data protection legislation and this policy. The DPO will:

- advise the school, governing body and staff on data protection requirements;
- monitor compliance;
- provide advice on Data Protection Impact Assessments;
- advise on data protection risks;
- support the school in responding to data protection rights requests;
- advise on personal data breaches;
- liaise with the ICO where appropriate;
- provide advice regarding contracts, data sharing and third-party suppliers;
- support staff training and awareness;
- advise on privacy notices and other data protection documentation; and
- maintain an appropriate level of professional expertise.

The DPO is the principal point of contact for data protection matters.
DPO provider: Judicium Education
Telephone: 0207 336 8403

Staff should contact the DPO when they are unsure about how personal data should be collected, used, shared, retained or secured.

5.3 Headteacher

The Headteacher is responsible for the day-to-day implementation of this policy and acts as the school's senior lead for data protection. The Headteacher will:

- ensure appropriate procedures are implemented;
- ensure staff receive appropriate training;
- ensure data protection risks are considered when introducing new systems or processes;
- work with the DPO to respond to breaches and rights requests;
- ensure appropriate action is taken following data protection incidents; and
- report significant issues to the Governing Body.

5.4 All staff

All staff are responsible for protecting personal data and must:

- comply with this policy and associated procedures;
- only access personal data necessary for their role;
- keep personal data secure;
- ensure information is accurate and up to date;
- not disclose personal data to unauthorised individuals;
- use school-approved systems to store and process personal data;
- report suspected data breaches immediately;
- complete required data protection training;
- follow the school's retention and disposal arrangements; and
- seek advice when unsure about any aspect of data protection.

Staff must contact the DPO where they:

- have concerns about compliance;
- are unsure whether processing is lawful;
- are considering a new use of personal data;
- are considering sharing personal data with another organisation;
- are introducing a new system, app, platform or technology;
- need advice about consent;
- receive a data protection rights request;
- identify a potential data breach;
- are considering transferring personal data outside the UK; or
- require advice about a contract involving personal data.

6. Data protection principles

The school will comply with the seven key data protection principles. Personal data must be:

1. Lawful, fair and transparent – processed in a lawful, fair and transparent manner.
2. Purpose limited – collected for specified, explicit and legitimate purposes.
3. Adequate and limited – adequate, relevant and limited to what is necessary.
4. Accurate – accurate and kept up to date where necessary.
5. Stored appropriately – kept for no longer than necessary.
6. Secure – processed in a way that ensures appropriate security.
7. Accountable – the school must be able to demonstrate compliance with these principles.

7. Lawful processing

The school will only process personal data where it has an appropriate lawful basis. The lawful bases available under data protection law include:

- consent;
- performance of a contract;
- compliance with a legal obligation;
- protection of vital interests;
- performance of a task carried out in the public interest or in the exercise of official authority; and
- legitimate interests, where applicable.

The school will identify and document the appropriate lawful basis for each significant processing activity. For tasks undertaken by the school in its capacity as a public authority, the school will generally rely on the public task/official authority or legal obligation lawful bases rather than legitimate interests. Where consent is used, it must be:

- freely given;
- specific;
- informed;
- unambiguous;
- capable of being withdrawn; and
- recorded by the school.

The school will not use consent where an individual does not have a genuine choice. For children's data, the school will consider the child's age, understanding, capacity and best interests when determining how information should be collected and how rights should be exercised. There is no general fixed age at which a child automatically has capacity to consent to the processing of their personal data in England. Capacity will depend on the circumstances and the child's understanding.

8. Special category data

Special category data requires additional protection. The school will only process special category data where:

1. an appropriate lawful basis under Article 6 UK GDPR applies; and
2. an appropriate condition for processing special category data under Article 9 UK GDPR and the Data Protection Act 2018 applies.

This may include processing relating to:

- safeguarding;
- health and medical information;
- SEND;
- equality and diversity;
- religious beliefs;
- dietary requirements;
- biometric identification;
- occupational health; and
- other information requiring additional protection.

Access to special category data will be limited to individuals who need the information to carry out their role.

9. Criminal offence data
Criminal offence data will only be processed where the school has:

- an appropriate lawful basis under Article 6 UK GDPR; and
- an additional condition permitted by Article 10 UK GDPR and the Data Protection Act 2018.

Where required, the school will maintain appropriate documentation and safeguards for such processing.

10. Privacy notices and transparency
The school will provide clear and accessible privacy notices explaining how personal data is used. Privacy notices will explain, where relevant:

- what personal information is collected;
- why it is collected;
- the lawful basis for processing;
- who information may be shared with;
- how long information will be retained;
- individuals' rights;
- how to contact the DPO;
- how to complain;
- information about international transfers;
- information about automated decision-making or profiling where applicable; and
- other information required by data protection law.

Privacy notices will be reviewed at least annually and whenever there is a significant change in the way personal data is processed. DfE guidance specifically expects schools to make their privacy notices freely available and to review them regularly.

11. Data minimisation, accuracy and purpose limitation
The school will only collect information that is necessary for a specific and legitimate purpose. Staff must not collect or retain information simply because it might be useful in the future. Personal data must:

- be relevant to the purpose for which it is collected;
- be accurate;
- be updated where necessary;
- only be accessed by those who need it; and
- be securely deleted or anonymised when no longer required.

Staff must inform the school promptly if their own personal information changes.

12. Sharing personal data
The school may share personal data where there is a lawful basis for doing so. Information may be shared with, for example:

- parents/carers and pupils where appropriate;
- the local authority;
- the Department for Education;
- Ofsted;
- other schools;
- social care;
- health services;
- safeguarding partners;
- police and other law enforcement agencies;
- examination and assessment organisations;
- educational psychologists and other professionals;
- payroll and HR providers;
- IT and educational technology providers;
- insurers and legal advisers; and
- other organisations where there is a lawful basis.

Consent is not automatically required before sharing information. In particular, safeguarding concerns may require information to be shared without consent where there is a lawful basis and this is necessary to protect a child or another person. The school will consider:

- the purpose of sharing;
- the lawful basis;
- whether the information is necessary and proportionate;
- whether only the minimum necessary information is shared;
- the security of the recipient;
- whether a data sharing agreement or other contractual safeguards are required; and
- whether a DPIA is required.

The DPO will be consulted where there is uncertainty about a proposed data sharing arrangement. DfE guidance emphasises that information should be shared appropriately where this is necessary to keep children safe, while ensuring that sharing is lawful, necessary and proportionate.

13. Data processors and third-party suppliers

Where an external organisation processes personal data on behalf of the school, the school will ensure appropriate due diligence has been completed. Before appointing a data processor, the school will consider:

- the supplier's data protection arrangements;
- security measures;
- the nature and volume of data processed;
- where data is stored;
- whether information is transferred internationally;
- retention and deletion arrangements;
- sub-processors;
- data breach procedures; and
- the supplier's ability to comply with data protection legislation.

Appropriate contractual arrangements will be put in place. The school will not use educational technology or other systems that process personal data without appropriate consideration of data protection requirements. Where a new technology or system is likely to result in a high risk to individuals, the school will complete a Data Protection Impact Assessment before processing begins. Current DfE guidance specifically expects schools to consider data protection by design and by default when procuring educational technology.

14. International transfers

The school will ensure that any transfer of personal data outside the UK complies with applicable UK data protection law. Before making an international transfer, the school will seek advice from the DPO and ensure that an appropriate transfer mechanism and safeguards are in place.

15. Children's personal data

The school recognises that children require particular protection in relation to their personal data. When processing children's information, the school will consider:

- the child's age and level of understanding;
- the nature and sensitivity of the information;
- the purpose of processing;
- the child's best interests;
- the risks to the child;
- the transparency of the processing; and
- the child's rights.

Information provided to children will be clear, accessible and age appropriate wherever appropriate.

16. Individual rights

Individuals have a number of rights under data protection law, although these rights are not all absolute. Depending on the circumstances, individuals may have the right to:

- be informed about how their personal data is used;
- access their personal data;
- have inaccurate data corrected;
- request erasure;
- request restriction of processing;
- object to certain processing;
- request data portability where applicable;
- withdraw consent where processing is based on consent;
- object to certain direct marketing;
- challenge certain solely automated decisions; and
- complain about the school's use of their personal data.

The school will respond to rights requests in accordance with statutory timescales and will seek advice from the DPO where necessary.

17. Subject Access Requests

An individual may make a Subject Access Request (SAR) to obtain access to their personal data. A SAR can be made verbally or in writing and does not need to use particular wording or a specific form. Staff

who receive a SAR must immediately pass it to the DPO or the member of staff responsible for coordinating information rights requests. The school may need to verify the identity of the requester where this is reasonable and necessary. The school will:

- respond without undue delay and normally within one month;
- provide information free of charge in most circumstances;
- consider whether an extension is permitted where a request is complex or numerous;
- identify information that may lawfully be withheld or redacted;
- consider the rights of other individuals whose information appears in the requested material; and
- document decisions about withholding or restricting information.

The one-month period begins when the school has received the request and has sufficient information to identify the requester where identity verification is necessary. The school will not routinely require individuals to use a specific form to make a SAR. Current ICO guidance confirms that a SAR may be made in a variety of ways.

18. Children's Subject Access Requests

A child has their own data protection rights. When a request is made by a parent or carer on behalf of a child, the school will consider:

- whether the child is sufficiently mature to understand the request;
- the child's wishes, where appropriate;
- whether the child has consented;
- the nature of the information requested;
- the child's best interests;
- whether the person making the request has parental responsibility; and
- any other relevant circumstances.

There is no automatic rule that a parent can access all of a child's personal data simply because they have parental responsibility. As a general guide, younger children may be less likely to understand the implications of a subject access request, while older children may be able to exercise their rights themselves. This will always be assessed on a case-by-case basis.

19. Requests for pupils' educational records

For maintained schools, parents have a separate legal right under the Education (Pupil Information) (England) Regulations 2005 to access their child's educational record. Where applicable, the school will make an educational record available for inspection or provide a copy within **15 school days** of receiving a written request. This right is separate from the right of access under data protection legislation. The school may withhold information where the law permits or requires it to do so. Current DfE assessment guidance confirms the 15-school-day requirement for maintained schools.

20. Complaints about data protection

Individuals who have concerns about how the school processes their personal data should contact the school or the DPO in the first instance. The school will provide accessible ways for individuals to raise data protection concerns, including an electronic means of making a complaint. Complaints will be:

- acknowledged appropriately;

- investigated fairly and promptly;
- responded to without undue delay; and
- recorded where appropriate.

Individuals also have the right to complain directly to the Information Commissioner's Office. The school will cooperate fully with the ICO where required. The Data (Use and Access) Act 2025 has strengthened requirements around data protection complaints, including requirements concerning accessible complaint mechanisms and acknowledgement of complaints.

21. Photographs and videos

The school may take photographs and videos of pupils and staff for legitimate school purposes. These may include:

- recording learning and school activities;
- safeguarding;
- assessment;
- displays within school;
- newsletters;
- school publications;
- the school website;
- social media;
- promotional materials;
- press coverage; and
- other educational or communication purposes.

The school will identify an appropriate lawful basis for each use. Where consent is relied upon, consent will be obtained before the relevant processing takes place and will be capable of being withdrawn. The school will explain how photographs and videos will be used and will avoid using unnecessary personal information alongside images. Parents/carers taking photographs or videos at school events for their own personal purposes should respect the privacy of other children and families and should not publish images of other pupils publicly without appropriate permission. Further information is contained in the school's Safer Use of Images Policy**.**

22. Artificial Intelligence

The school recognises that generative AI can provide educational and administrative benefits but may also create significant data protection risks. Staff, governors and pupils must not enter personal, confidential, safeguarding or special category information into an AI tool unless the tool has been approved by the school and appropriate data protection checks have been completed. Staff must:

- only use school-approved AI tools for school business;
- avoid entering personal data wherever possible;
- check how the tool processes and stores information;
- follow the school's acceptable use requirements;
- not upload confidential documents without authorisation;
- consider whether a DPIA is required;
- check AI-generated content for accuracy; and
- report any suspected disclosure of personal data immediately.

The school will consider data protection, safeguarding, security, age restrictions and transparency when introducing AI systems. Where personal data is proposed for use within an AI system, the school will consult the DPO and IT lead before implementation. Current DfE guidance recommends that personal data is not used in generative AI tools unless this is necessary and appropriate safeguards are in place. The school will also consider the implications of AI systems that involve profiling or automated decision-making. Where automated decision-making is used, the school will ensure appropriate safeguards and human oversight are in place as required by current data protection law.

23. Filtering and monitoring

The school uses appropriate filtering and monitoring systems to support the safeguarding of pupils and staff. Monitoring information will be:

- collected for clear and legitimate purposes;
- accessed only by authorised individuals;
- handled securely;
- retained only for an appropriate period; and
- managed in accordance with safeguarding and data protection requirements.

Where monitoring systems identify concerns, information may be shared with appropriate staff or external agencies where there is a lawful basis. The school will ensure that staff who have access to monitoring information receive appropriate training.

A DPIA will be completed before introducing a new filtering or monitoring system or making significant changes to an existing system where required.

The school's privacy notice will explain relevant filtering and monitoring arrangements. Current DfE guidance specifically requires schools to consider what is monitored, why, who can access information and how long it is retained.

24. Data protection by design and default

The school will consider data protection at the earliest stage of any new project, system, policy or process involving personal data. This includes:

- introducing new software or educational technology;
- changing how pupil or staff information is collected;
- introducing monitoring systems;
- implementing biometric systems;
- sharing information with new organisations;
- using AI;
- changing assessment systems; and
- introducing new online services.

Where processing is likely to result in a high risk to individuals, a Data Protection Impact Assessment will be completed. The DPO will advise on whether a DPIA is required. The school will use privacy-friendly settings wherever possible and will only collect and process information that is necessary.

25. Data security
The school will implement appropriate technical and organisational measures to protect personal data. These may include:

- password protection;
- multi-factor authentication where available and appropriate;
- encryption;
- access controls;
- secure school networks;
- antivirus and security software;
- secure cloud systems;
- locked filing cabinets;
- secure disposal;
- staff training;
- appropriate filtering and monitoring;
- regular security updates; and
- procedures for responding to incidents.

Staff must:

- lock computers when unattended;
- use strong, unique passwords;
- not share passwords;
- not use personal email accounts for school business;
- not store school personal data on unauthorised personal devices;
- not use unauthorised cloud storage;
- take care when sending emails containing personal information;
- check recipients before sending information;
- use secure methods when transferring sensitive information; and
- report suspected phishing, malware or other cyber incidents promptly.

The school will ensure that access to personal data is based on role and legitimate need.

26. Paper records and information taken off site
Paper records containing personal data must be stored securely when not in use. Confidential information must not be left:

- on desks;
- in classrooms;
- in staffrooms;
- in vehicles;
- in reception areas; or
- in other locations where unauthorised individuals could access it.

Where personal information must be taken away from school premises, staff must:

- take only the minimum information necessary;
- ensure it is appropriately protected;

- use secure school-approved devices where electronic information is involved; and
- return or securely dispose of information when it is no longer required.

27. Personal devices
Staff must not store personal or confidential school information on personal devices unless this has been specifically authorised and appropriate security measures are in place. Where personal devices are authorised for school purposes, staff must comply with the school's acceptable use, online safety and information security requirements. Personal data must not be transferred to personal email accounts or unauthorised cloud storage.

28. Retention and disposal of records
The school will retain personal data only for as long as it is necessary for the purpose for which it was collected or where there is a legal or regulatory requirement to retain it. The school will maintain a Records Retention Schedule identifying appropriate retention periods. Retention periods will take account of:

- statutory requirements;
- safeguarding considerations;
- educational requirements;
- legal claims;
- financial and accounting requirements;
- employment requirements; and
- operational needs.

The school will review records periodically and securely dispose of information that is no longer required. DfE guidance expects schools to maintain appropriate retention arrangements and to check periodically whether information is still required.

29. Disposal of personal data
Personal data will be disposed of securely. Paper records will be:

- shredded;
- securely destroyed; or
- disposed of through an appropriately contracted confidential waste provider.

Electronic records will be securely deleted or destroyed where appropriate. Where a third party disposes of personal data on behalf of the school, appropriate contractual and security arrangements will be in place.

30. Personal data breaches
A personal data breach may include:

- sending an email to the wrong recipient;
- losing a laptop or mobile device;
- losing paper records;
- accidental disclosure of safeguarding information;
- publishing personal data on the school website;
- unauthorised access to school systems;

- phishing or cyber attacks;
- sharing information with an unauthorised person;
- inappropriate use of AI;
- theft of personal information; or
- accidental deletion or destruction of personal data.

All suspected breaches must be reported immediately to the DPO/Headteacher.

Staff must not attempt to conceal a breach. The school will:

1. contain the breach;
2. establish what happened;
3. identify the information and individuals affected;
4. assess the risks;
5. take steps to reduce potential harm;
6. determine whether the breach must be reported to the ICO;
7. notify affected individuals where legally required;
8. record the breach and the decision-making process; and
9. take action to prevent recurrence.

Where a breach is reportable, the school will notify the ICO without undue delay and, where feasible, within 72 hours of becoming aware of it**.** All personal data breaches will be recorded, whether or not they are reported to the ICO.

31. Data breach reporting procedure
Any member of staff, governor, volunteer or contractor who discovers or suspects a personal data breach must immediately inform:

<u>Headteacher / Data Protection Officer</u>
They should provide as much information as possible about:

- what happened;
- when it happened;
- what information was involved;
- who may have received or accessed it;
- who may be affected;
- what action has already been taken; and
- whether the information has been recovered.

The person reporting the incident should not delay reporting while attempting to establish all the facts.

The DPO will coordinate the investigation and risk assessment. The school will document:

- the facts of the incident;
- its effects;
- the risk assessment;
- actions taken;
- decisions about notification;

- communications with affected individuals;
- communications with the ICO, where applicable; and
- steps taken to prevent recurrence.

32. Examples of data breaches
Examples include:

Email sent to the wrong person
If confidential or sensitive information is emailed to the wrong recipient, the sender must immediately report this to the DPO and, where possible, attempt to recall or contain the message. The DPO will assess the risk and determine appropriate action.

Lost or stolen device
A lost or stolen school laptop, tablet or phone must be reported immediately. The school will take steps to secure accounts, remotely disable or erase the device where possible and assess whether personal data has been compromised.

Misfiled pupil information
If a report or document containing personal information is given to the wrong pupil or family, this must be reported immediately.

Unauthorised AI disclosure
If personal or confidential information is entered into an unauthorised AI system, this must be treated as a potential data breach and reported immediately.

Published personal information
If personal information is accidentally published on the school website, social media or another public platform, the school will remove the information as quickly as possible and assess the potential impact.

33. Data protection training
All staff and governors will receive data protection training as part of induction. Training will be refreshed periodically and whenever there are significant changes to:

- legislation;
- school procedures;
- technology;
- cyber security risks;
- AI use; or
- data protection requirements.

Training will include, where appropriate:
- data protection principles;
- confidentiality;
- information security;
- phishing and cyber security;
- data breaches;
- children's data;
- safeguarding information;

- subject access requests;
- appropriate data sharing;
- use of photographs;
- AI and personal data; and
- retention and secure disposal.

The school will maintain records of training completed.

34. Monitoring and review
The Headteacher, supported by the DPO, will monitor compliance with this policy. Monitoring may include:

- data protection audits;
- review of data breaches;
- review of subject access requests;
- review of complaints;
- staff training records;
- supplier checks;
- review of privacy notices;
- review of retention arrangements;
- DPIA records;
- review of data sharing arrangements; and
- review of school systems and security arrangements.

The policy will be reviewed annually and sooner where there are significant changes to legislation, ICO or DfE guidance, school systems or processing activities. The Governing Body will approve the policy.

35. Links with other policies
This policy should be read alongside the school's:

- Child Protection and Safeguarding Policy;
- Online Safety Policy;
- Acceptable Use Policy;
- Freedom of Information Policy;
- Safer Use of Images Policy;
- Records Retention Schedule;
- Cyber Security / Information Security procedures;
- Complaints Policy;
- CCTV Policy or procedures;
- Staff Code of Conduct;
- Data Breach Procedure; and
- AI / Generative AI guidance, where applicable.

Appendix 1: Personal Data Breach Procedure

Step 1 – Report
Report the incident immediately to the Headteacher/DPO.
Do not wait until all the facts are known.

Step 2 – Contain
Take immediate reasonable steps to prevent further disclosure or loss.
Examples include:

- recalling an email;
- contacting the unintended recipient;
- recovering paper records;
- disabling an account;
- changing passwords;
- remotely locking a device;
- removing information from a website; or
- contacting the IT provider.

Step 3 – Assess
The DPO will assess:

- what information is involved;
- how sensitive it is;
- how many people are affected;
- who may have accessed it;
- whether children or vulnerable individuals are affected;
- the likelihood of harm;
- the seriousness of potential harm; and
- what mitigation has been possible.

Step 4 – Decide whether notification is required
The DPO will determine whether the breach must be reported to the ICO.
Where required, notification will be made without undue delay and, where feasible, within 72 hours of the school becoming aware of the breach.

If the breach is likely to result in a high risk to individuals, the school will consider whether the affected individuals must also be informed without undue delay.

Step 5 – Record
Every personal data breach will be recorded, whether or not it is reported to the ICO.
The record will include:

- date and time;
- nature of the breach;
- information involved;
- individuals affected;
- likely consequences;

- actions taken;
- mitigation;
- notification decisions; and
- lessons learned.

Step 6 – Learn and improve
Following a breach, the Headteacher and DPO will consider:

- why the breach occurred;
- whether procedures were followed;
- whether further staff training is required;
- whether systems need to be changed;
- whether access arrangements should be amended; and
- whether similar risks exist elsewhere in the school.

Appendix 2: Staff – What to do if you are unsure
Before collecting, using or sharing personal data, staff should ask:

1. Do I need this information?
Only collect and use information that is necessary.
2. Am I authorised to access it?
Only access information needed for your role.
3. Do I have a lawful basis?
If unsure, contact the DPO.
4. Does the information contain sensitive or confidential information?
If yes, take additional care.
5. Am I sharing it with the right person?
Check recipients carefully before sending.
6. Am I using an approved system?
Do not upload school information to unauthorised apps, websites or AI tools.
7. Do I need to keep it?
Follow the school's retention arrangements.
8. Has something gone wrong?
Report it immediately. Do not wait and do not try to hide it.

Appendix 3: Data Protection Officer

Data Protection Officer: Judicium Education
Telephone: 0207 336 8403

Staff should contact the DPO for advice regarding:

- data protection compliance;
- data breaches;
- subject access requests;
- data sharing;
- DPIAs;
- privacy notices;
- contracts and suppliers;
- international data transfers;
- AI and personal data;
- children's data protection rights; and
- any other data protection concern.