Glebe School

Data Protection & Information Management Policy

Date approved by Trustees	
Date of next review	Summer 2024

CONTENTS

Statement of Intent

Glebe School is required to keep and process certain information about its staff members, pupils, trustees and other third parties, the school is therefore a data controller and is registered with the Information Commissioner's Office (ICO). The school keeps and processes data in accordance with its legal obligations under the Data Protection Act 2018 (DPA 2018) and the General Data Protection Regulation (GDPR).

The school may, from time to time, be required to share personal information about its staff, pupils, trustees or third parties with other organisations, mainly the LA, Department for Education, other schools and educational bodies, children's services and other third parties, such as payroll providers or IT services.

This policy is in place to ensure all staff and trustees are aware of their responsibilities and outlines how the school complies with the following core principles of the GDPR.

Organisational methods for keeping data secure are imperative, and Glebe School believes that it is good practice to keep clear practical policies, backed up by written procedures.

1. Legal framework

1.1 This policy has due regard to legislation, including, but not limited to the following:

- The Data Protection Act 2018
- The General Data Protection Regulation (GDPR)
- The Freedom of Information Act 2000
- The Education (Pupil Information) (England) Regulations 2005 (as amended in 2016)
- The Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004
- The School Standards and Framework Act 1998

1.2 This policy will also have regard to guidance published by the Information Commissioner's Office guidance on the DPA 2018 and the GDPR.

1.3 This policy will be implemented in conjunction with the following other school policies, including:

- E-safety Policy/IT Acceptable Use Policy
- Pupil Remote/Blended Learning Policy
- Staff Code of Conduct
- Disciplinary Policy & Procedures
- Parental Photography Policy

2. Applicable data

2.1 For the purpose of this policy, **personal data** refers to information that relates to an identifiable, living individual, including information such as an online identifier, e.g. an IP address. The GDPR applies to both automated personal data and to manual filing systems, where personal data is accessible according to specific criteria, as well as to chronologically ordered data and pseudonymised data, e.g. key-coded.

2.2 **Sensitive personal data** is referred to in the GDPR as 'special categories of personal data', which are broadly the same as those that were specified in the Data Protection Act (DPA) 1998. These specifically include the processing of genetic data, biometric data and data concerning health matters.

3. Principles

3.1 In accordance with the requirements outlined in the GDPR, personal data will be:

- Processed lawfully, fairly and in a transparent manner in relation to individuals.
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
- Accurate and, where necessary, kept up-to-date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods, insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals.
- 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.

3.2 The GDPR also requires that "the controller shall be responsible for, and able to demonstrate, compliance with the principles".

4. Accountability

4.1 Glebe School will implement appropriate technical and organisational measures to demonstrate that data is processed in line with the principles set out in the GDPR.

4.2 The school will provide comprehensive, clear and transparent privacy policies.

4.3 Records of activities relating to higher risk processing will be maintained, such as the processing of special categories data or that in relation to criminal convictions and offences.

4.4 Internal records of processing activities will include the following:

- Name and details of the organisation
- Purpose(s) of the processing
- Description of the categories of individuals and personal data
- Retention schedules
- Categories of recipients of personal data
- Description of technical and organisational security measures
- Details of transfers to third countries where applicable, including documentation of the transfer mechanism safeguards in place

4.5 The school will implement measures that meet the principles of data protection by design and data protection by default, such as:

- Data minimisation.

- Pseudonymisation.
- Transparency.
- Allowing individuals to monitor processing.
- Continuously creating and improving security features.

4.6 Data protection impact assessments will be used, where appropriate.

5. Data protection officer (DPO)

5.1 A DPO will be appointed in order to:

- Inform and advise the school and its employees about their obligations to comply with the GDPR and other data protection laws.
- Monitor the school's compliance with the GDPR and other laws, including managing internal data protection activities, advising on data protection impact assessments, conducting internal audits, and providing the required training to staff members.

5.2 The individual appointed as DPO will have professional experience and knowledge of data protection law, particularly that in relation to schools.

5.3 The DPO will report to the highest level of management at the school, which is the Head Teacher.

5.4 The DPO will operate independently and will not be dismissed or penalised for performing their task.

5.5 Sufficient resources will be provided to the DPO to enable them to meet their GDPR obligations.

5.6 Where the DPO role is performed by an individual external to the school, a senior employee will be appointed to the role of data protection lead to manage information processes onsite, to support the role of DPO and advise management and trustees. The school's data protection lead is the School Business Manager.

5.7 The school's DPO service is currently provided by:

Cantium Business Solutions (working with Invicta Law Ltd.)
Worrall House
West Malling,
Kent
ME14 1XQ

DPO email: dpo@invicta.law
DPO contact no: 01622 392051

6. Lawful processing

6.1 The legal basis for processing data will be identified and documented prior to data being processed.

6.2 Under the GDPR, data will be lawfully processed under the following conditions:

- The consent of the data subject has been obtained.
- Processing is necessary for:
  - The data needs to be processed so that the school can comply with a **legal obligation**.
  - The data needs to be processed so that the school, as a public authority, can perform a task in the **public interest** or exercise its official authority.

- The data needs to be processed so that the school can fulfil a **contract** with the data subject, or the data subject has asked the school to take specific steps before entering into a contract.
- The data needs to be processed to ensure the **vital interests** of the individual or another person i.e. to protect someone's life.
- The data needs to be processed for the **legitimate interests** of the school (where the processing is not for any tasks the school performs as a public authority) or a third party, provided the individual's rights and freedoms are not overridden. (This condition is not available to processing undertaken by the school in the performance of its tasks.)

6.3 Sensitive data and criminal offence data will only be processed under the following conditions:

- Explicit consent of the data subject, unless reliance on consent is prohibited by law.
- Processing carried out by a not-for-profit body with a political, philosophical, religious or trade union aim provided the processing relates only to members or former members (or those who have regular contact with it in connection with those purposes) and provided there is no disclosure to a third party without consent.
- Processing relates to personal data manifestly made public by the data subject.
- Processing is necessary for:
  - Carrying out obligations under employment, social security or social protection law, or a collective agreement.
  - Protecting the vital interests of a data subject or another individual where the data subject is physically or legally incapable of giving consent.
  - The establishment, exercise or defence of legal claims or where courts are acting in their judicial capacity.
  - Reasons of substantial public interest on the basis of UK law which is proportionate to the aim pursued and which contains appropriate safeguards.
  - The purposes of preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or management of health or social care systems and services on the basis of UK law or a contract with a health professional.
  - Reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of healthcare and of medicinal products or medical devices.
  - Archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes in accordance with Article 89(1).

7. Consent

7.1 Consent must be a positive indication. It cannot be inferred from silence, inactivity or pre-ticked boxes.

7.2 Consent will only be accepted where it is freely given, specific, informed and an unambiguous indication of the individual's wishes.

7.3 Where consent is given, a record will be kept documenting how and when consent was given.

7.4 The school ensures that consent mechanisms meet the standards of the GDPR. Where the standard of consent cannot be met, an alternative legal basis for processing the data must be found, or the processing must cease.

7.5 Consent accepted under the DPA will be reviewed to ensure it meets the standards of the GDPR; however, acceptable consent obtained under the DPA will not be reobtained.

7.6 Consent can be withdrawn by the individual at any time.

7.7 Where a child is under the age of 16 or younger if the law provides it (up to the age of 13), the consent of parents will be sought prior to the processing of their data, except where the processing is related to preventative or counselling services offered directly to a child.

7.8 In all other instances with regards to obtaining consent, an appropriate age of consent is considered by the school on a case-by-case basis, taking into account the requirements outlined in 7.2.

8. The right to be informed

8.1 The privacy notice supplied to individuals in regards to the processing of their personal data will be written in clear, plain language which is concise, transparent, easily accessible and free of charge.

8.2 If services are offered directly to a child, the school will ensure that the privacy notice is written in a clear, plain manner that the child will understand.

8.3 In relation to data obtained both directly from the data subject and not obtained directly from the data subject, the following information will be supplied within the privacy notice:

- The identity and contact details of the controller (and where applicable, the controller's representative) and the DPO.
- The purpose of, and the legal basis for, processing the data.
- The legitimate interests of the controller or third party.
- Any recipient or categories of recipients of the personal data.
- Details of transfers to third countries if applicable and the safeguards in place.
- The retention period or criteria used to determine the retention period.
- The existence of the data subject's rights, including the right to:
  - Withdraw consent at any time.
  - Lodge a complaint with a supervisory authority.
- The existence of automated decision making, including profiling, how decisions are made, the significance of the process and the consequences.

8.4 Where data is obtained directly from the data subject, information regarding whether the provision of personal data is part of a statutory or contractual requirement, as well as any possible consequences of failing to provide the personal data, will be provided.

8.5 Where data is not obtained directly from the data subject, information regarding the categories of personal data that the school holds, the source that the personal data originates from and whether it came from publicly accessible sources, will be provided.

8.6 For data obtained directly from the data subject, this information will be supplied at the time the data is obtained.

8.7 In relation to data that is not obtained directly from the data subject, this information will be supplied:

- Within one month of having obtained the data.
- If disclosure to another recipient is envisaged, at the latest, before the data is disclosed.
- If the data is used to communicate with the individual, at the latest, when the first communication takes place.

9. The right of access

9.1 Individuals have the right to obtain confirmation that their data is being processed.

9.2 Individuals have the right to submit a Subject Access Request (SAR) to gain access to their personal data in order to verify the lawfulness of the processing.

9.3 The SAR can be submitted in any form but we may be able to respond more quickly where a submission is made in writing and includes the name, contact number, address, email address and details of the information requested.

9.4 The school will verify the identity of the person making the request before any information is supplied. The school may ask the person to provide 2 forms of identification.

9.5 A copy of the information will be supplied to the individual free of charge; however, the school may impose a 'reasonable fee' to comply with requests for further copies of the same information.

9.6 Where a SAR has been made electronically, the information will be provided in a commonly used electronic format.

9.7 Where a request is manifestly unfounded, excessive or repetitive, a reasonable fee will be charged.

9.8 All fees will be based on the administrative cost of providing the information.

9.9 All requests will be responded to without delay and at the latest, **within one month** of receipt (or receipt of the additional information needed to confirm identity, where relevant.)

9.10 In the event of numerous or complex requests, the period of compliance will be extended by a further two months. The individual will be informed of this extension, and will receive an explanation of why the extension is necessary, within one month of the receipt of the request.

9.11 Where a request is manifestly unfounded or excessive, the school holds the right to refuse to respond to the request. The individual will be informed of this decision and the reasoning behind it, as well as their right to complain to the supervisory authority and to a judicial remedy, within one month of the refusal.

9.12 In the event that a large quantity of information is being processed about an individual, the school will ask the individual to specify the information the request is in relation to.

9.13 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 SAR with respect to their child, the child must either be unable to understand their rights and the implications of a SAR, or have given their consent.

9.14 Children below the age of 12 are generally not regarded to be mature enough to understand their rights and the implications of a SAR. Therefore, most SARs from parents or carers of pupils at our school may be granted without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

9.15 We may not disclose information for a variety of reasons, such as if it:

- Might cause serious harm to the physical or mental health of the pupil or another individual.

- Would reveal that the child is being or has been abused, or 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.

9.16 When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO or they can seek to enforce their subject access right through the courts.

10. Parental requests to see the educational record

10.1 Parents, or those with parental responsibility, have a legal right to free access to their child's educational record (which includes most information about a pupil) within 15 days of a written request. If the request is for a copy of the record the school may charge a fee to cover the cost of supplying it. This right applies as long as the child concerned is aged under 18.

10.2 There are certain circumstances in which this right can be denied, such as if releasing the information might cause serious harm to the physical or mental health of the pupil or another individual, or if it would mean releasing exam marks before they are officially announced.

11. The right to rectification

11.1 Individuals are entitled to have any inaccurate or incomplete personal data rectified.

11.2 Where the personal data in question has been disclosed to third parties, the school will inform them of the rectification where possible.

11.3 Where appropriate, the school will inform the individual about the third parties that the data has been disclosed to.

11.4 Requests for rectification will be responded to **within one month**; this will be extended by two months where the request for rectification is complex.

11.5 Where no action is being taken in response to a request for rectification, the school will explain the reason for this to the individual, and will inform them of their right to complain to the supervisory authority and to a judicial remedy.

12. The right to erasure

12.1 Individuals hold the right to request the deletion or removal of personal data where there is no compelling reason for its continued processing.

12.2 Individuals have the right to erasure in the following circumstances:

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed
- When the individual withdraws their consent
- When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing
- The personal data was unlawfully processed

- The personal data is required to be erased in order to comply with a legal obligation
- The personal data is processed in relation to the offer of information society services to a child

12.3 The school has the right to refuse a request for erasure where the personal data is being processed for the following reasons:

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

12.4 As a child may not fully understand the risks involved in the processing of data when consent is obtained, special attention will be given to existing situations where a child has given consent to processing and they later request erasure of the data, regardless of age at the time of the request.

12.5 Where personal data has been disclosed to third parties, they will be informed about the erasure of the personal data, unless it is impossible or involves disproportionate effort to do so.

12.6 Where personal data has been made public within an online environment, the school will inform other organisations who process the personal data to erase links to and copies of the personal data in question.

13. The right to restrict processing

13.1 Individuals have the right to block or suppress the school's processing of personal data.

13.2 In the event that processing is restricted, the school will store the personal data, but not further process it, guaranteeing that just enough information about the individual has been retained to ensure that the restriction is respected in future.

13.3 The school will restrict the processing of personal data in the following circumstances:

- Where an individual contests the accuracy of the personal data, processing will be restricted until the school has verified the accuracy of the data
- Where an individual has objected to the processing and the school is considering whether their legitimate grounds override those of the individual
- Where processing is unlawful and the individual opposes erasure and requests restriction instead
- Where the school no longer needs the personal data but the individual requires the data to establish, exercise or defend a legal claim

13.4 The school will inform individuals when a restriction on processing has been lifted.

14. The right to data portability

14.1 Individuals have the right to obtain and reuse their personal data for their own purposes across different services.

14.2 Personal data can be easily moved, copied or transferred from one IT environment to another in a safe and secure manner, without hindrance to usability.

14.3 The right to data portability only applies in the following cases:

- To personal data that an individual has provided to a controller
- Where the processing is based on the individual's consent or for the performance of a contract
- When processing is carried out by automated means

14.4 Personal data will be provided in a structured, commonly used and machine-readable form.

14.5 The school will provide the information free of charge.

14.6 Where feasible, data will be transmitted directly to another organisation at the request of the individual.

14.7 The school is not required to adopt or maintain processing systems which are technically compatible with other organisations.

14.8 In the event that the personal data concerns more than one individual, the school will consider whether providing the information would prejudice the rights of any other individual.

14.9 The school will respond to any requests for portability **within one month**.

14.10 Where the request is complex, or a number of requests have been received, the timeframe can be extended by two months, ensuring that the individual is informed of the extension and the reasoning behind it within one month of the receipt of the request.

14.11 Where no action is being taken in response to a request, the school will, without delay and at the latest within one month, explain to the individual the reason for this and will inform them of their right to complain to the supervisory authority and to a judicial remedy.

15. The right to object

15.1 The school will inform individuals of their right to object at the first point of communication, and this information will be outlined in the privacy notice and explicitly brought to the attention of the data subject, ensuring that it is presented clearly and separately from any other information.

15.2 Individuals have the right to object to the following:

- Processing based on legitimate interests or the performance of a task in the public interest
- Direct marketing
- Processing for purposes of scientific or historical research and statistics.

15.3 Where personal data is processed for the performance of a legal task or legitimate interests:

- An individual's grounds for objecting must relate to his or her particular situation.
- The school will stop processing the individual's personal data unless the processing is for the establishment, exercise or defence of legal claims, or, where the school can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual.

15.4 Where personal data is processed for direct marketing purposes:

- The school will stop processing personal data for direct marketing purposes as soon as an objection is received.
- The school cannot refuse an individual's objection regarding data that is being processed for direct marketing purposes.

15.5 Where personal data is processed for research purposes:

- The individual must have grounds relating to their particular situation in order to exercise their right to object.
- Where the processing of personal data is necessary for the performance of a public interest task, the school is not required to comply with an objection to the processing of the data.

15.6 Where the processing activity is outlined above, but is carried out online, the school will offer a method for individuals to object online.

16. Automated decision making and profiling

16.1 Individuals have the right not to be subject to a decision when:

- It is based on automated processing, e.g. profiling.
- It produces a legal effect or a similarly significant effect on the individual.

16.2 The school will take steps to ensure that individuals are able to obtain human intervention, express their point of view, and obtain an explanation of the decision and challenge it.

16.3 When automatically processing personal data for profiling purposes, the school will ensure that the appropriate safeguards are in place, including:

- Ensuring processing is fair and transparent by providing meaningful information about the logic involved, as well as the significance and the predicted impact.
- Using appropriate mathematical or statistical procedures.
- Implementing appropriate technical and organisational measures to enable inaccuracies to be corrected and minimise the risk of errors.
- Securing personal data in a way that is proportionate to the risk to the interests and rights of the individual and prevents discriminatory effects.

16.4 Automated decisions must not concern a child or be based on the processing of sensitive data, unless:

- The school has the explicit consent of the individual.
- The processing is necessary for reasons of substantial public interest on the basis of Union/Member State law.

17. Privacy by design and privacy impact assessments

17.1 The school will act in accordance with the GDPR by adopting a privacy by design approach and implementing technical and organisational measures which demonstrate how the school has considered and integrated data protection into processing activities.

17.2 Data protection impact assessments (DPIAs) will be used to identify the most effective method of complying with the school's data protection obligations and meeting individuals' expectations of privacy.

17.3 DPIAs will allow the school to identify and resolve problems at an early stage, thus reducing associated costs and preventing damage from being caused to the school's reputation which might otherwise occur.

17.4 A DPIA will be carried out when using new technologies or when the processing is likely to result in a high risk to the rights and freedoms of individuals.

17.5 A DPIA will be used for more than one project, where necessary.

17.6 High risk processing includes, but is not limited to, the following:

- Systematic and extensive processing activities, such as profiling
- Large scale processing of special categories of data or personal data which is in relation to criminal convictions or offences
- The use of CCTV

17.7 The school will ensure that all DPIAs include the following information (see Appendix 1):

- A description of the processing operations and the purposes
- An assessment of the necessity and proportionality of the processing in relation to the purpose
- An outline of the risks to individuals
- The measures implemented in order to address risk

17.8 Where a DPIA indicates high risk data processing, the school will consult the ICO to seek its opinion as to whether the processing operation complies with the GDPR.

18. Data breaches

18.1 The term 'personal data breach' refers to a breach of security which has led to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

18.2 The Head Teacher will ensure that all staff members are made aware of, and understand, what constitutes a data breach as part of their induction & CPD training.

18.3 Staff must report any data breach or potential breach as soon as possible to the School Business Manager or Head Teacher. Data breaches are recorded by the School Business Manager and are reported to the DPO.

18.4 Where a breach is likely to result in a risk to the rights and freedoms of individuals, the relevant supervisory authority will be informed.

18.5 All notifiable breaches will be reported to the relevant supervisory authority within 72 hours of the school becoming aware of it.

18.6 The risk of the breach having a detrimental effect on the individual, and the need to notify the relevant supervisory authority, will be assessed on a case-by-case basis.

18.7 In the event that a breach is likely to result in a high risk to the rights and freedoms of an individual, the school will notify those concerned directly. The notification will be made in writing and will include the contact details of the school and the DPO, a clear description of the breach, the likely consequences and the steps taken to mitigate any adverse effects.

18.8 A 'high risk' breach means that the threshold for notifying the individual is higher than that for notifying the relevant supervisory authority.

18.9 In the event that a breach is sufficiently serious, the public will be notified without undue delay.

18.10 Effective and robust breach detection, investigation and internal reporting procedures are in place at the school, which facilitate decision-making in relation to whether the relevant supervisory authority or the public need to be notified.

18.11 Within a breach notification, the following information will be outlined:

- The nature of the personal data breach, including the categories and approximate number of individuals and records concerned
- The name and contact details of the DPO
- An explanation of the likely consequences of the personal data breach
- A description of the proposed measures to be taken to deal with the personal data breach
- Where appropriate, a description of the measures taken to mitigate any possible adverse effects

18.12 Failure to report a breach when required to do so may result in a fine, as well as a fine for the breach itself.

19. Data security

19.1 Confidential paper records will be kept in a locked filing cabinet, drawer or safe, with restricted access.

19.2 Confidential paper records will not be left unattended or in clear view anywhere with general access.

19.3 Digital data both on a local hard drive and on the school's network is password-protected. The network drive is backed up daily off-site.

19.4 Access to the school's network is controlled and access to sensitive and confidential data on the network is restricted to only those members of staff who require the information to perform their duties effectively.

19.5 Access to the school's management information system SIMS is password-protected and access to sensitive and confidential data on SIMS is restricted to only those members of staff who require the information to perform their duties effectively.

19.6 Staff are not permitted to use removable storage e.g. external hard drives, except where permission is granted by a member of the SLT and appropriate measures are put in place to keep the device secure.

19.7 Staff are permitted to use password-protected and fully encrypted memory sticks ONLY when permission is granted by SLT for purposes where no ther method is workable.

19.8 such as work moderation where an exam board accepts no other means. In these instances, memory sticks will be provided by the school

19.9 All electronic devices are password-protected to protect the information on the device in case of theft. Electronic devices are kept securely when not in use, e.g. in a locked cabinet.

19.10 Devices holding pupil and staff photos will be regularly wiped to delete all images. Memory cards will be kept in a locked cabinet when not in use and will be wiped regularly.

19.11 Where possible, the school will use software which enables remote blocking or deletion of data in case of theft.

19.12 Staff, trustees and student teachers are permitted to use their personal laptops or computers for school purposes but must only access school personal or confidential data via the secure remote working solution provided or though LGFL secure email or on an encrypted memory stick. No school personal or confidential data must be saved onto personal devices.

19.13 Where a member of staff works offsite using a school device, they must ensure that the device is password protected and they must not permit the school device to be used by any other person, e.g. family member or friend.

19.14 All members of staff are provided with their own secure login and password for the school's network, and every computer regularly prompts users to change their password.

19.15 Staff, trustees, student teachers or volunteers (where appropriate) must not use personal email addresses for sharing or viewing any school data. Secure LGFL email accounts can be provided for all staff trustees, student teachers or volunteers (where appropriate).

19.16 Emails containing sensitive or confidential information must be sent by secure mail service (e.g. Egress).Sensitive documents must be password-protected or sent by OneDrive if there are unsecure servers between the sender and the recipient

19.17 Circular emails to parents/students are sent blind carbon copy (bcc), so email addresses are not disclosed to other recipients.

19.18 When sending confidential information, staff will always check that the recipient is correct before sending.

19.19 No personal data or sensitive personal data must be shared by text or on social media e.g. Whatsapp. See also the school's e-Safety and IT Acceptable Use Policy.

19.20 Where personal information that could be considered private or confidential is taken off the premises, either in electronic or paper format, staff will take extra care to follow the same procedures for security, e.g. keeping devices or paperwork under lock and key. The person taking the information from the school premises accepts full responsibility for the security of the data.

19.21 Before sharing data, all staff members will ensure:

- They are allowed to share it.
- That adequate security is in place to protect it.
- The person or organisation who will receive the data has been outlined in a privacy notice.
- The person or organisation who will receive the data have confirmed in writing that they comply with the GDPR and any other relevant data protection legislation.

19.22 Under no circumstances are volunteers, visitors or unauthorised third parties allowed access to confidential or personal information. Those visiting areas of the school containing sensitive information are supervised at all times. Where third parties will have access to data, e.g. student teachers, school photographer, a confidentiality agreement will be signed and retained. (see appendix 4)

19.23 The physical security of the school's buildings and storage systems, and access to them, is reviewed on a regular basis. If an increased risk in vandalism/burglary/theft is identified, extra measures to secure data storage will be put in place.

19.24 Glebe School takes its duties under the GDPR seriously and any unauthorised disclosure may result in disciplinary action, in accordance with the school's Disciplinary Policy & Procedure.

19.25 The School Business Manager (SBM) is responsible for business continuity and recovery measures are in place to ensure the security of protected data.

20. Publication of information

20.1 Glebe School publishes a publication scheme on its website (see Appendix 2) outlining classes of information that will be made routinely available, including:
Policies and procedures
Annual reports
Financial information, such as Pupil Premium Grant

20.2 Classes of information specified in the publication scheme are made available quickly and easily on request.

20.3 Glebe School will not publish any personal information, including photos, on its website without the permission of the affected individual.

20.4 When uploading information to the school website, staff are considerate of any metadata or deletions which could be accessed in documents and images on the site.

21. Remote Learning & Working

21.1 The Remote/Blended Learning Policy details our approach to managing data processed as a result of online learning activities and virtual lessons and meetings.

21.2 All personal data processed as a result of online learning and working will be handled in line with data protection legislation.

21.3 Staff must only access school personal or confidential data via the secure remote working solution provided or though LGFL secure email. No school personal or confidential data must be saved onto personal devices.

21.4 Where a member of staff works offsite using a school device, they must sign and comply with the school's device loan agreement (Appendix 3), including ensuring that the device is password protected and not permitting the school device to be used by any other person, e.g. family member or friend.

22. CCTV and photography

22.1 The school understands that recording images of identifiable individuals constitutes processing personal information, so it is done in line with data protection principles. Please, see the school's Digital Media and Images Consent Form for more details.

22.2 The school, as the corporate body, is the data controller digital imagery. The Board of Trustees of Glebe School therefore has overall responsibility for ensuring that records are maintained, including security and access arrangements in accordance with regulations.

22.3 The school uses a closed digital CCTV system which does not record audio. The system is registered with the ICO in line with data protection legislation. Warning signs have been placed throughout the premises where the surveillance system is active, as mandated by the ICO's Code of Practice.

22.4 The purpose for collecting CCTV images is communicated via this policy which is available on the website.The school will only use surveillance cameras for the safety, welfare and security of the school and its staff, pupils and visitors. Surveillance will be used as a deterrent for violent behaviour, damage to the school and criminal activity.

22.5 The school will only conduct surveillance as a deterrent and under no circumstances will the surveillance and the CCTV cameras be present in school classrooms or any changing facility or where they intrude on anyone's privacy.

22.6 All CCTV footage will be kept for 30 days for security purposes; the SBM is responsible for keeping the records secure and allowing access. Only where there may be a child protection or safeguarding issue, can footage be kept longer; specifically for this purpose.

22.7 Access to the surveillance system, software and data will be strictly limited to authorised operators and will be password protected.

22.8 The surveillance system may be used to assist the police in identifying persons who have committed an offence.

22.9 The school will always indicate its intentions for taking photographs of pupils and will obtain permission before publishing them.

22.10 If the school wishes to use images/video footage of pupils in a publication, such as the school website, prospectus, or recordings of school plays, written permission will be sought for the particular usage from the parent or pupil, where he/she has capacity to consent.

22.11 Under the UK GDPR, individuals have the right to obtain confirmation that their personal information is being processed. Individuals have the right to submit an SAR to gain access to their personal data in order to verify the lawfulness of the processing. Requests by persons outside the school for viewing or copying photographs, disks, or obtaining digital recordings, will be assessed by the School Business Manager, who will consult the Data Protection Officer, on a case-by-case basis with close regard to data protection and freedom of information legislation.

22.12 Images captured by individuals for recreational/personal purposes, and videos made by parents for family use, are exempt from the GDPR. However, we will ask that parents/carers comply with the school's Parental Photography Policy and that photos or videos with other pupils in them are not shared publicly on social media for safeguarding reasons, unless all the relevant parents/carers (or pupils where appropriate) have agreed to this.

23. Data retention

23.1 Data will not be kept for longer than is necessary. The school follows the Information Commissioner's guidance on retention of documents, including the Information and Records Management Society's Retention Guidelines for Schools.

23.2 Unrequired data will be deleted as soon as practicable.

23.3 Some educational records relating to former pupils or employees of the school may be kept for an extended period for legal reasons, but also to enable the provision of references or academic transcripts.

23.4 Paper documents will be shredded or pulped, and electronic memories scrubbed clean or destroyed, once the data should no longer be retained.

23.5 Emails will be deleted from the system after 2 years.

23.6 When a member of staff leaves the employment of the school, their email account and personal drive on the school server will normally be deleted after 3 months, unless there are exceptional circumstances for retaining the account and this is authorised by the Headteacher or School Business Manager.

24. DBS data

24.1 All data provided by the DBS will be handled in line with data protection legislation; this includes electronic communication.

24.2 Any third parties who access DBS information will be made aware of the data protection legislation, as well as their responsibilities as a data handler.

25. Freedom of Information

25.1 As an educational provider, our school has an obligation to publish a freedom of information statement, outlining how we will meet our duties under the Freedom of Information Act 2000 and associated regulations. The development and effective implementation of this policy fulfils that requirement.

25.2 The school will follow the guidance published by the ICO for public organisations at: https://ico.org.uk/for-organisations/guide-to-freedom-of-information/

25.3 This policy outlines our school's policy and procedures for:

- The release and publication of private data and public records.
- Providing applicants with advice and assistance throughout the duration of their requests.
- It also clarifies our position regarding the appropriate limit to the costs incurred by the school in obtaining any requested information, and on charging fees for its provision.

25.4 The school will only accept a request for information which meets all of the following criteria:

- It is in writing (this includes requests sent to the school's official social media accounts).
- It states the name of the applicant (not a pseudonym) and an address for correspondence.
- It is in English, or is translated into English at the applicant's expense
- It adequately describes the information requested.

25.5 A request will be treated as made in writing if it meets all of the following requirements:

- It is transmitted by electronic means.
- It is received in legible form.
- It is capable of being used for subsequent reference.

25.6 Requests should be posted to the school or emailed to admin@glebe.bromley.sch.uk and marked for the attention of the School Business Manager.

25.7 Provided that the request meets the requirements set out above in this policy, the school will comply with its duty to:

- Confirm or deny to any person making a request for information to the school, whether it holds information of the description specified in the request.

- Provide the documentation, if the school confirms that it holds the requested information.

25.8 The duties outlined above will be completed no later than 20 school days, or 60 working days if this is shorter, from receipt of the request.

25.9 The information provided to the applicant will be in the format that they have requested, where possible. Where it is not possible to provide the information in the requested format, the school will assist the applicant by discussing alternative formats in which it can be provided.

25.10 The school may, within 20 school days, give an applicant who has requested information from the school, a written notice stating that a fee is to be charged for the school's compliance. Charges may be made for costs and disbursements, such as the following:

- Production expenses, e.g. printing and photocopying.
- Transmission costs, e.g. postage.
- Complying with the applicant's preferences about the format in which they would like to receive the information, e.g. scanning to a CD.
- Costs related to the time spent by any person undertaking activities to locate and process the data, are to be estimated at a rate of £25 per person per hour.

25.11 Where a fee is charged, the timeframe within which the school has to respond to the request begins from the day the fee is received. The school will not comply with any freedom of information request that exceeds the statutorily imposed appropriate limit of £450.

25.12 The school will not comply with a request where:

- The school reasonably requires further information to meet a freedom of information request, has informed the applicant of this requirement, but was not subsequently supplied with that further information.
- The information is no longer readily available as it is contained in files that have been placed in archive storage or is difficult to access for similar reasons.
- A request for information is exempt under section 2 of the Freedom of Information Act 2000.
- The cost of providing the information exceeds the appropriate limit.
- The request is vexatious.
- The request is a repeated request from the same person made within 60 consecutive working days of the initial one.
- A fee notice was not honoured, within 3 months of issue.
- The requested information is not held by the school for the purposes of the school's business.

25.13 If information falls within scope of a qualified exemption and the school needs additional time to consider the public interest test, the school may extend the deadline. In most cases, the extension will exceed no more than a further 20 school days; however, the actual length of the extension will be decided on a case-by-case basis and the applicant will be informed.

25.14 The school will meet its duty to provide advice and assistance, as far as is reasonable, to any person who proposes to make, or has made, requests for information to the school. The school may offer advice and assistance in the following circumstances:

- If an individual requests to know what types of information the school holds and the format in which it is available, as well as information on the fees regulations and charging procedures.
- If a request has been made, but the school is unable to regard it as a valid request due to insufficient information, leading to an inability to identify and locate the information.
- If a request has been refused, e.g. due to an excessive cost, and it is necessary for the school to assist the individual who has submitted the request.

25.15 The school will provide assistance for each individual on a case-by-case basis; examples of how the school will provide assistance include the following:

- Informing an applicant of their rights under the Freedom of Information Act 2000.

- Assisting an individual in the focus of their request, e.g. by advising of the types of information available within the requested category.
- Advising an applicant if information is available elsewhere and how to access this information.
- Keeping an applicant informed on the progress of their request.

25.16 The school will meet its duty to adopt and maintain a publication scheme which specifies the information which it will publish on the school's website, and whether the information will be available free of charge or on payment, see the publication scheme at Appendix 2. The publication scheme will be reviewed and, where necessary, updated every 2 years.

26. Policy review

26.1 This policy will be reviewed by the Head Teacher every 2 years, or in light of any changes to relevant legislation.

Appendix 1

Data Protection Impact Assessment

Introduction

- Project name
- Explain what the project aims to achieve, and what the benefits will be to the school, to individuals and to other members of the school community.
- Link to any other relevant documents related to the project, e.g. a project proposal.
- Describe the process for the collection and deletion of any personal data.
- Explain what information will be used used, what it is used for and who will have access to it.
- Detail how many individuals are likely to be affected by the project.

Question	Yes	No	Unsure	Comments
Will the project involve collecting new information about individuals?				
Will the project require individuals to provide information about themselves?				
Will information about individuals be disclosed to other individuals or organisations who have not previously held information about the individual?				
Is any information about individuals held for purposes it is not currently used for, or in a way it is not currently used?				
Will the project involve using a new technology that might be perceived as being intrusive to an individual's privacy?				
Will the project result in any decisions or actions taken against individuals which may have a significant impact on them?				
Will any information about individuals raise privacy concerns, e.g. information they may wish to keep private, such as criminal information held on DBS certificates?				
Will the project require you to contact individuals in ways that they may find intrusive?				

Risk Assessment

Potential Risk	Risk Rate H/M/L	Proposed Solutions	Responsibility	Risk reduced to acceptable level Y/N
Risk to individuals				
For example: 1. Transparency - individuals are not aware that their data is being processed, how, or for what purposes 2. Accuracy – data is not accurate and, where necessary, kept up-to-date 3. Personal data breach – destruction, loss, alteration, unauthorized disclosure/access of the individuals data 4. Data being shared with third party who do not process lawfully or hold data securely		Privacy notice issued to individual Specify how data will be collected, reviewed and updated Security measure in place – password protection, encrypted devices etc Written agreement in place with third party		
Risk to school				
For example: 1. Accuracy – data used for project is not correct 2. Data breach > reputational damage 3. Data breach > may lead to a sanction imposed by the Information Commissioner's Office				
Risk to compliance with GDPR				
For example: 1. Data is not processed fairly and lawfully 2. Where consent is required (e.g. for photos) it was not freely given, specific,				

informed and an unambiguous 3. Data is not collected for specified, explicit and legitimate purposes 4. Data is not adequate, relevant and limited to what is necessary 5. Kept in a form which permits identification of data subjects for no longer than is necessary 6. Right to deletion – new software/system does not permit amending or deleting information to comply with retention periods				

Appendix 2

Publication scheme

This scheme follows the model approved by the Information Commissioner and sets out the classes of information which we publish or intend to publish; the format in which the information will be made available and whether the information is available free of charge or on payment.

1. Classes of information

Information that is available under this scheme includes:

- Who we are and what we do
- What we spend and how we spend it
- What are our priorities are and how we are doing
- How we make decisions
- Our policies and procedures
- The services we offer

Information which **will not** be made available under this scheme includes:

- Information the disclosure of which is prevented by law, or exempt under the Freedom of Information Act, or is otherwise properly considered to be protected from disclosure.
- Information in draft form.
- Information that is no longer readily available as it is contained in files that have been placed in archive storage, or is difficult to access for similar reasons.

2. Information available on our website

Every academy, free school and college should publish specific information on its website to comply with their funding agreement.

The information we publish is as follows:

1. School or college contact details (required)
2. Admission arrangements (required)
3. Ofsted reports (required)
4. Exam and assessment results (annual report/pupil outcomes)
5. Performance tables
6. Curriculum
7. Behaviour policy
8. Pupil premium (required)
9. Equality objectives (required)
10. Special educational needs and disabilities – SEND (required)
11. Careers programme information
12. Complaints policy (required)
13. Annual reports and accounts
14. Executive pay (required for all posts with remuneration £100,000+ per annum)
15. Trustees' information and duties (required)
16. Charging and remissions policies
17. Values and ethos

Requested documents under the publication scheme will be delivered electronically where possible, but paper copies can be provided by contacting the school using the below contact details.

To enable us to process your request quickly, please mark all correspondence:
"FREEDOM OF INFORMATION REQUEST for the Attention of the School Business Manager" and email to admin@glebe.bromley.sch.uk

Documents can be translated under disability legislation into accessible formats where possible.

3. Charges

Documents contained in this scheme are free to view on the school website or single paper copies are available free of charge to parents and prospective parents of the school who request them.

4. Feedback

We welcome any comments or suggestions you may have regarding this scheme. Please contact the school, for the attention of the School Business Manager, using the below contact details:

admin@glebe.bromley.sch.uk

0208 777 4540

Appendix 3:

Device loan agreement for Staff at Glebe School

1. The agreement:

Governs the use and care of devices assigned to staff. This agreement covers the period from the date the device is issued through to the return date of the device to the school.
All issued equipment shall remain the sole property of Glebe School and is governed by the school's policies.
1. The school is lending the member of staff a laptop for the purpose of doing work from home.
2. This agreement sets out the conditions for taking a Glebe School laptop home.
I confirm that I have read the terms and conditions set out in the agreement and my signature at the end of this agreement confirms that I will adhere to the terms of loan.

2. Damage/loss

By signing this agreement I agree to take full responsibility for the loan equipment issued to me and I understand the conditions of the agreement.
I understand that I am responsible for the equipment at all times whether on the school's property or not.
If the equipment is damaged, lost or stolen, I will immediately inform IT Support at Glebe School, and I acknowledge that I am responsible for the reasonable costs requested by the school to repair or replace the equipment. If the equipment is stolen, I will also immediately inform the police.
I agree to keep the equipment in good condition and to return it to the school at their request, in the same condition.
I will not leave the equipment unsupervised in unsecured areas.
I will make sure I take the following measures to protect the device:

- Keep the device in a secure place when not in use
- Don't leave the device in a car or on show at home
- Don't eat or drink around the device
- Don't lend the device to any other person
- Don't leave the equipment unsupervised in unsecured areas

3. Unacceptable use

I am aware that the school monitors the activity on this device.
I agree that I will not carry out any activity that constitutes 'unacceptable use'.
This includes, but is not limited to the following:

- Using ICT or the internet to bully or harass someone else, or to promote unlawful discrimination
- Any illegal conduct, or statements which are deemed to be advocating illegal activity
- Activity which defames or disparages the school, or risks bringing the school into disrepute
- Causing intentional damage to ICT facilities or materials
- Using inappropriate or offensive language
- Accessing material and content which is in appropriate

I accept that the school may sanction me, in line with our Staff Code of Conduct, Disciplinary and IT Policies, if I engage in any of the above **at any time.**

4. Personal use

I agree that I will only use this device for work purposes and not for personal use and will not loan the equipment to any other person.

5. Data protection

I agree to take the following measures to keep the data on the device protected.

- Make sure I lock the equipment if it's left inactive for a period of time
- Do not share the equipment among family or friends
- Update antivirus and anti-spyware software as required.
- Install the latest updates to operating systems, as prompted.

If I need help doing any of the above, I will contact IT support at Glebe school on the email:
itsupport@glebe.bromley.sch.uk

6. Return date

I will return the device in its original condition to Glebe School/IT support dept when requested to do so.
I will return the device at the end of the Covid-19 lockdown period, or as requested to do so at any time by a member of the school's management team.
I will also ensure the return of the equipment to the school if I leave the employment of the school.

7. Consent

By signing this form, I confirm that I have read and agree to the terms and conditions set out above.

STAFF FULL NAME	
STAFF SIGNATURE	
TYPE OF DEVICE E.G. LAPTOP	
SERIAL NUMBER OF DEVICE	

The signature can be typed if being returned by email.

Appendix 4:

Confidentiality and Non-Disclosure Statement
name of company

As a data controller, Glebe School has a responsibility to protect its personal data in line with the Data Protection Act 1998 and the General Data Protection Regulations (GDPR) which came into force on 25th May 2018. Therefore, the appropriate confidentiality and security requirements must be agreed.

Each student/ visitor from name of company/ tutor must comply with the following:

- Use the data the school discloses to you for the specific service it was provided and not for any other purpose or purposes unless agreed by the school.
- Only ask for school's personal data that is adequate and relevant to the task at hand so you can carry out services to Glebe School.
- Only hold school's personal data disclosed to you for as long as agreed by Glebe School. When no longer needed, you must ensure you always securely destroy data in line with The Data Protection Act 1998 and the General Data Protection Regulations (GDPR).
- You must take all appropriate technical and physical measures to protect the personal data you are holding on behalf of Glebe School. For example: electronic personal data must not be held on an un-encrypted device and ensuring that all electronic systems are protected. If you are accessing paper records, they must be transported from one location to another securely.
- You must not share the school's personal data we disclose to you with any other third parties without the consent of Glebe School unless you are permitted to by law.
- In addition, for support functions that Glebe School do not directly enter into contract with but may become party to it, it is your responsibility to ensure those support functions keep schools personal data confidential and secured at all times.
- Under no circumstances will the school's personal data you are collecting be transferred outside of the European Economic Area (EEA).
- At the end of any work placement/ visit, data and school property, e.g. entry fobs, must be returned to Glebe School.

To ensure best practice, it is advisable to extend this advice to any third parties you work with or may work with when handling schools personal data. This is to ensure that the confidentiality of personal data is upheld.

Unlawful disclosure or selling of personal information

Under The Data Protection Act 1998 and General Data Protection Regulation (GDPR) is it a criminal offence to sell or disclose personal data 'knowingly or recklessly' to anyone you are not supposed to, therefore, any inappropriate or unauthorised disclosure of the schools personal information could be subject to legal action.

I ..... **have read and understood the above statement**

Signed: ..... **Date:** .....