



Goldington Green Academy

Data Protection Policy

General Data Protection Regulation (GDPR).

Date: January 2019

Person Responsible for Policy: Headteacher

Date of Approval: May 2018

Approved By: Staffing Committee

Cycle of Review: Every 3 years Date Next

Review is Required: Spring 2022

Contents:

[Statement of intent](#)

1. [Legal framework](#)
2. [Applicable data](#)
3. [Principles](#)
4. [Accountability](#)
5. [Data protection officer \(DPO\)](#)
6. [Lawful processing](#)
7. [Consent](#)
8. [The right to be informed](#)
9. [The right of access](#)
10. [The right to rectification](#)
11. [The right to erasure](#)
12. [The right to restrict processing](#)
13. [The right to data portability](#)
14. [The right to object](#)
15. [Automated decision making and profiling](#)
16. [Privacy by design and privacy impact assessments](#)
17. [Data breaches](#)
18. [Data security](#)
19. [Publication of information](#)
20. [Photography](#)
21. [Data retention](#)
22. [DBS data](#)
23. [Policy review](#)
24. [Appendix 1](#)
25. [Appendix 2](#)

Statement of intent

Goldington Green Academy is required to keep and process certain information including personal data about its staff members and pupils in accordance with its legal obligations under the General Data Protection Regulation (GDPR).

The school may, from time to time, be required to share personal information about its staff, governors or pupils with other organisations, mainly the LA, other schools and educational bodies, and potentially children's services.

This policy is in place to ensure all staff and governors 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 Goldington Green Academy believes that it is good practice to keep clear practical policies, backed up by written procedures.

This policy complies with the requirements set out in the GDPR, which will come into effect on 25 May 2018. The government have confirmed that the UK's decision to leave the EU will not affect the commencement of the GDPR.

1. Legal framework

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

- 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 the following guidance:

- Information Commissioner's Office (2017) 'Overview of the General Data Protection Regulation (GDPR)'
- Information Commissioner's Office (2017) 'Preparing for the General Data Protection Regulation (GDPR) 12 steps to take now'

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

- **Use of Photographs & Video Policy**
- **E-safety acceptable user policy**
- **Freedom of Information Policy**

2. Applicable data

2.1. For the purpose of this policy, **personal data** refers to information that relates to an identifiable, living individual. 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 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. Goldington Green Academy 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 notices.
- 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, 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. An existing employee will be appointed to the role of DPO provided that their duties are compatible with the duties of the DPO and do not lead to a conflict of interests.
- 5.3. The individual appointed as DPO will have professional experience and knowledge of data protection law, particularly that in relation to schools.
- 5.4. The DPO will report to the highest level of management at the school, which is the headteacher.
- 5.5. The DPO will operate independently and will not be dismissed or penalised for performing their task.
- 5.6. Sufficient resources will be provided to the DPO to enable them to meet their GDPR obligations.

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:
 - Compliance with a legal obligation.
 - The performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.
 - For the performance of a contract with the data subject or to take steps to enter into a contract.
 - Protecting the vital interests of a data subject or another person.
 - For the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject. (This condition is not available to processing undertaken by the school in the performance of its tasks.)
 - The individual (or their parent/carer when appropriate in the case of a pupil) has freely given clear consent
- 6.3. Sensitive data will only be processed under the following conditions:
- Explicit consent of the data subject, unless reliance on consent is prohibited by EU or Member State 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 Union or Member State 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 Union or Member State 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. 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.

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. 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.
 - The retention period of 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.
- 8.3. 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.
- 8.4. 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.
- 8.5. For data obtained directly from the data subject, this information will be supplied at the time the data is obtained.
- 8.6. 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 are disclosed.
 - If the data are 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 school will verify the identity of the person making the request before any information is supplied.
- 9.4. 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.

- 9.5. Where a SAR has been made electronically, the information will be provided in a commonly used electronic format.
- 9.6. Where a request is manifestly unfounded, excessive or repetitive, a reasonable fee will be charged.
- 9.7. All fees will be based on the administrative cost of providing the information.
- 9.8. All requests will be responded to without delay and at the latest, within one month of receipt.
- 9.9. 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.
- 9.10. 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.
- 9.11. 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.

10. The right to rectification

- 10.1. Individuals are entitled to have any inaccurate or incomplete personal data rectified.
- 10.2. Where the personal data in question has been disclosed to third parties, the school will inform them of the rectification where possible.
- 10.3. Where appropriate, the school will inform the individual about the third parties that the data has been disclosed to.
- 10.4. Requests for rectification will be responded to within one month; this will be extended by two months where the request for rectification is complex.
- 10.5. 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.

11. The right to erasure

- 11.1. Individuals hold the right to request the deletion or removal of personal data where there is no compelling reason for its continued processing.
- 11.2. 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
- 11.3. 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
- 11.4. 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.
- 11.5. 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.
- 11.6. 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.

12. The right to restrict processing

- 12.1. Individuals have the right to block or suppress the school's processing of personal data.
- 12.2. 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.
- 12.3. 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
- 12.4. If the personal data in question has been disclosed to third parties, the school will inform them about the restriction on the processing of the personal data, unless it is impossible or involves disproportionate effort to do so.
- 12.5. The school will inform individuals when a restriction on processing has been lifted.

13. The right to data portability

- 13.1. Individuals have the right to obtain and reuse their personal data for their own purposes across different services.
- 13.2. 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.
- 13.3. 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
- 13.4. Personal data will be provided in a structured, commonly used and machine-readable form.
- 13.5. The school will provide the information free of charge.
- 13.6. Where feasible, data will be transmitted directly to another organisation at the request of the individual.
- 13.7. The school is not required to adopt or maintain processing systems which are technically compatible with other organisations.
- 13.8. 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.
- 13.9. The school will respond to any requests for portability within one month.

13.10. 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.

13.11. 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.

14. The right to object

14.1. 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.

14.2. 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.

14.3. 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.

14.4. 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.

14.5. 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.

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

15. Automated decision making and profiling

15.1. 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.

15.2. 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.

15.3. 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.

15.4. 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.

16. Privacy by design and privacy impact assessments

16.1. 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.

16.2. 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.

- 16.3. 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.
- 16.4. 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.
- 16.5. A DPIA will be used for more than one project, where necessary.
- 16.6. 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.
- 16.7. The school will ensure that all DPIAs include the following information:
 - 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
- 16.8. 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.

17. Data breaches – see Appendix 1

- 17.1. 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.
- 17.2. The headteacher will ensure that all staff members are made aware of, and understand, what constitutes a data breach as part of their CPD training.
- 17.3. Where a breach is likely to result in a risk to the rights and freedoms of individuals, the relevant supervisory authority will be informed.
- 17.4. All notifiable breaches will be reported to the relevant supervisory authority within 72 hours of the school becoming aware of it.
- 17.5. 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.
- 17.6. 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.

- 17.7. A 'high risk' breach means that the threshold for notifying the individual is higher than that for notifying the relevant supervisory authority.
- 17.8. In the event that a breach is sufficiently serious, the public will be notified without undue delay.
- 17.9. 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.
- 17.10. 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
- 17.11. Failure to report a breach when required to do so may result in a fine, as well as a fine for the breach itself.

18. Data security

- 18.1. Confidential paper records will be kept in a locked filing cabinet, drawer or safe, with restricted access.
- 18.2. Confidential paper records will not be left unattended or in clear view anywhere with general access.
- 18.3. Digital data is coded, encrypted or password-protected, both on a local hard drives and on a network drives and are regularly backed up and taken off-site.
- 18.4. Where data is saved on removable storage or a portable device, the device will be kept in a locked filing cabinet, drawer or safe when not in use.
- 18.5. Memory sticks will not be used.
- 18.6. All electronic devices are password-protected to protect the information on the device in case of theft.
- 18.7. Staff and governors will not use their personal laptops or computers for school purposes unless they are personally password-protected and fully encrypted.

- 18.8. All necessary members of staff are provided with their own secure login and password, and every computer regularly prompts users to change their password.
- 18.9. Emails containing sensitive or confidential information are password-protected if there are unsecure servers between the sender and the recipient.
- 18.10. Circular emails to parents are sent blind carbon copy (bcc), so email addresses are not disclosed to other recipients.
- 18.11. When sending confidential information by fax, staff will always check that the recipient is correct before sending.
- 18.12. 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 under lock and key. The person taking the information from the school premises accepts full responsibility for the security of the data.
- 18.13. Before sharing data, all staff members will ensure:
- They are allowed to share it.
 - That adequate security is in place to protect it.
 - Who will receive the data has been outlined in a privacy notice.
- 18.14. Under no circumstances are visitors allowed access to confidential or personal information. Visitors to areas of the school containing sensitive information are supervised at all times.
- 18.15. The physical security of the school's buildings and storage systems, and access to them, is reviewed on a termly basis. If an increased risk in vandalism/burglary/theft is identified, extra measures to secure data storage will be put in place.
- 18.16. Goldington Green Academy takes its duties under the GDPR seriously and any unauthorised disclosure may result in disciplinary action.
- 18.17. The school business manager (SBM) is responsible for continuity and recovery measures are in place to ensure the security of protected data.

19. Publication of information

- 19.1. Goldington Green Academy publishes on its website information that is made routinely available, including:
- Policies and procedures
 - Minutes of meetings
 - Annual reports
 - Financial information

- 19.2. Goldington Green Academy will not publish any personal information, including photos, on its website without the permission of the affected individual or if it is a child their parents.
- 19.3. 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.

20. Photography

- 20.1. The school understands that recording images of identifiable individuals constitutes as processing personal information, so it is done in line with data protection principles.
- 20.2. The school will always indicate its intentions for taking photographs of pupils and will retrieve permission before publishing them.
- 20.3. 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 of the pupil via the "Consent form for photography or videoing in school " signed when the child joins the school.
- 20.4. Precautions, as outlined in the Policy for the Use of Photographs and video, are taken when publishing photographs of pupils, in print, video or on the school website.
- 20.5. Images captured by individuals for recreational/personal purposes, and videos made by parents for family use, are exempt from the GDPR.

21. Data retention – see Appendix 2

- 21.1. Data will not be kept for longer than is necessary.
- 21.2. Unrequired data will be deleted as soon as practicable.
- 21.3. 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.
- 21.4. Paper documents will be shredded and electronic memories scrubbed clean or destroyed, once the data should no longer be retained.

22. DBS data

- 22.1. All data provided by the DBS will be handled in line with data protection legislation; this includes electronic communication.
- 22.2. Data provided by the DBS will never be duplicated.
- 22.3. 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.

Appendix 1: Personal data breach procedure

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

- On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the DPO
- The DPO will investigate the report, and determine whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidentally or unlawfully:
 - Lost
 - Stolen
 - Destroyed
 - Altered
 - Disclosed or made available where it should not have been
 - Made available to unauthorised people
- The DPO will alert the headteacher and the chair of governors
- The DPO will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary. (Actions relevant to specific data types are set out at the end of this procedure)
- The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen
- The DPO will work out whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the DPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:
 - Loss of control over their data
 - Discrimination
 - Identify theft or fraud
 - Financial loss
 - Unauthorised reversal of pseudonymisation (for example, key-coding)
 - Damage to reputation
 - Loss of confidentiality
 - Any other significant economic or social disadvantage to the individual(s) concerned

If it is likely that there will be a risk to people's rights and freedoms, the DPO must notify the ICO.

- The DPO will document the decision (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored in the DPO's data breach folder. The DPO will use a data breach log form.
- Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website within 72 hours. As required, the DPO will set out:
 - A description of the nature of the personal data breach including, where possible:

- The categories and approximate number of individuals concerned
 - The categories and approximate number of personal data records concerned
- The name and contact details of the DPO
- A description of the likely consequences of the personal data breach
- A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned
- If all the above details are not yet known, the DPO will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible
- The DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPO will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:
 - The name and contact details of the DPO
 - A description of the likely consequences of the personal data breach
 - A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned
- The DPO will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies
- The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:
 - Facts and cause
 - Effects
 - Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)

Records of all breaches will be stored in the DPO's data breach folder,

- The DPO and headteacher will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible

Actions to minimise the impact of data breaches

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

Sensitive information being disclosed via email (including safeguarding records)

- *If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error*

- *Members of staff who receive personal data sent in error must alert the sender and the DPO as soon as they become aware of the error*
- *If the sender is unavailable or cannot recall the email for any reason, the DPO will ask the ICT department to recall it*
- *In any cases where the recall is unsuccessful, the DPO will contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way*
- *The DPO will carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted*

A school laptop containing non-encrypted sensitive personal data being stolen or hacked

- *Inform the Police*
- *Follow the data breach procedure*

Appendix 2: Retention periods for records

Children's records	Retention period	Status	Authority
Children's records - including registers, medication record books and accident record books pertaining to the children	Until the child reaches the age of 21 - or until the child reaches the age of 24 for child protection records	Recommendation	Limitation Act 1980 Normal limitation rules (which mean that an individual can claim for negligently caused personal injury up to 3 years after, or deliberately caused personal injury up to 6 years after the event) are postponed until a child reaches 18 years of age
Records of any reportable death, injury, disease or dangerous occurrence	3 years after the date the record was made	Requirement	The Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 1995 (RIDDOR) (as amended)
Personnel records	Retention period	Status	Authority
Personnel files and training records (including disciplinary records and working time records)	6 years after employment ceases	Recommendation	Chartered Institute of Personnel and Development

DBS check	6 months	Recommendation	<p>DBS Code of Practice</p> <p>The following basic information should be retained after the certificate is destroyed: the date of issue; the name of the subject; the type of disclosure; the position for which the disclosure was requested; the unique reference number; and the details of the recruitment decision taken</p>
<i>Pay</i>			
Wage/salary records (including overtime, bonuses and expenses)	6 years	Requirement	Taxes Management Act 1970
Statutory Maternity Pay (SMP) records	3 years after the end of the tax year to which they relate	Requirement	The Statutory Maternity Pay (General) Regulations 1986
Statutory Sick Pay (SSP) records	3 years after the end of the tax year to which they relate	Requirement	The Statutory Sick Pay (General) Regulations 1982

Income tax and National Insurance returns/records	At least 3 years after the end of the tax year to which they relate	Requirement	The Income Tax (Employments) Regulations 1993 (as amended)
Redundancy details, calculations of payments, refunds, notification to the Secretary of State	3 years after employment ends	Recommendation	Chartered Institute of Personnel and Development
<i>Health and safety</i>			
Staff accident records (for organisations with 10 or more employees)	3 years after the date the record was made (there are separate rules for the recording of accidents involving hazardous substances)	Requirement	Social Security (Claims and Payments) Regulations 1979
Records of any reportable death, injury, disease or dangerous occurrence	3 years after the date the record was made	Requirement	The Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 1995 (RIDDOR) (as amended)

Accident/medical records as specified by the Control of Substances Hazardous to Health Regulations (COSHH) Asbestos.	40 years from the date of the last entry	Requirement	The Control of Substances Hazardous to Health Regulations 2002 (COSHH)
Assessments under Health and Safety Regulations and records of consultations with safety representatives and committees	Permanently	Recommendation	Chartered Institute of Personnel and Development
Financial records	Retention period	Status	Authority
Accounting records	3 years from the end of the financial year for private companies, 6 years for public	Requirement	Companies Act 2006
	limited companies		
	6 years for charities	Requirement	Charities Act 2011
Administrati on records	Retention period	Status	Authority
Employers' liability insurance records	For as long as possible	Recommendation	Health and Safety Executive
	10 years from		

Minutes/minute books	the date of the meeting for companies	Requirement	Companies Act 2006
	6 years from the date of the meeting for Charitable Incorporated Organisations	Requirement	The Charitable Incorporated Organisations (General) Regulations 2012