GDPR: Data Protection Policy

Goodwyn School (including EYFS)

This policy covers all pupils at Goodwyn School including the Early Years Foundation Stage (EYFS)

Statement and scope of the policy

Goodwyn School collects and uses certain types of personal information about staff, pupils, parents and other individuals who come into contact with the School in order to provide education and associated functions.

In order to carry out our ordinary duties to staff, pupils and parents, we process a wide range of personal data about individuals (including current, past and prospective staff, pupils or parents) as part of our daily operation.

The School may be required by law to collect and use certain types of information to comply with statutory obligations related to employment, education and safeguarding, and this policy is intended to ensure that personal information is dealt with properly and securely and in accordance with the General Data Protection Regulation ("GDPR"), the Data Protection Act 2018 and other related legislation.

Contents:

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:

- On Line safety Policy

2. Personal data

2.1. Personal data' is information that identifies an individual, and includes information that would identify an individual to the person to whom it is disclosed because of any special knowledge that they have or can obtain. A sub-set of personal data is known as 'special category personal data'. This special category data is information that reveals:

- race or ethnic origin;
- political opinions;
- religious or philosophical beliefs;
- trade union membership;
- physical or mental health;
- an individual's sex life or sexual orientation;
- genetic or biometric data for the purpose of uniquely identifying a natural person

2.2. Special Category Data is given special protection, and additional safeguards apply if this information is to be collected and used.

2.3. Information relating to criminal convictions shall only be held and processed where there is legal authority to do so.

3. Data Protection Principles

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

- will be processed fairly, lawfully and in a transparent manner, and processing shall not be lawful unless one of the processing conditions can be met;
- will be collected for specific, explicit, and legitimate purposes, and shall not be further processed in a manner incompatible with those purposes;
- shall be adequate, relevant, and limited to what is necessary for the purpose(s) for which it is being processed;
- shall be accurate and, where necessary, kept up to date;
- processed for any purpose(s) shall not be kept in a form which permits identification of individuals for longer than is necessary for that purpose/those purposes;
- shall be processed in such a way that ensures appropriate security of the data, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organisational measures.

4. Accountability

4.1. Goodwyn will implement appropriate technical and organisational measures to demonstrate that data is processed in line with the principles set out in section 3 above.

4.2. The school will provide comprehensive, clear and transparent privacy policies to inform individuals about how and why we process their personal data.

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. Lawful processing

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

5.2. The school will act as a data processor; however, this role may also be undertaken by other third parties.

5.3. 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.)

5.4. 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).

6. Use of Personal Data by Goodwyn School

6.1 The School processes personal data on pupils, staff and other individuals such as visitors. In each case, the personal data must be treated in accordance with the data protection principles as outlined in paragraph 3 above.

Pupils and Parents

6.2. The personal data held regarding pupils and parents is used in order to support the education of the pupils, to monitor and report on their progress, to provide appropriate pastoral care, and to assess how well the School as a whole is doing, together with any other uses normally associated with this provision in a school environment, including:

- For the purposes of pupil admission (and to confirm the identity of prospective pupils and their parents);
- To provide education services, including musical education, education, spiritual development, extra-curricular activities to pupils and monitoring pupils' progress and educational needs;
- Maintaining relationships with parents, pupils and the wider School community;
- For the purposes of management planning and forecasting, research and statistical analysis, including that imposed or provided for by law, market analysis and assessing pupil and parent satisfaction;
- To enable relevant authorities to monitor the School's performance and to intervene or assist with incidents as appropriate;
- To give and receive information and references about past, current and prospective pupils, including relating to outstanding fees or payment history, to/from any educational institution that the pupil attended or where it is proposed they attend.
- To enable pupils to take part in national or other assessments, and to publish the results of public examinations or other achievements of pupils of the school;
- To safeguard pupils' welfare and provide appropriate pastoral care;

- To monitor (as appropriate) use of the school's IT and communications systems in accordance with the school's On Line Safety policy;
- To make use of photographic images of pupils in school publications and on the School website in accordance with the School's policy on taking, storing and using images of children;
- For safety and security purposes, including CCTV, in accordance with the Information Commissioner's Office (ICO) Code of Practice;
- For maintenance of historic archive; and
- Where otherwise reasonably necessary for the School's purposes, including to obtain appropriate professional advice and insurance for the school.

Staff

6.3. The personal data of staff is used for the purposes of:

- Staff recruitment and appointment, including statutory recruitment checks and to confirm the identity of prospective staff. The data is used to comply with legal obligations placed on the School in relation to employment, and the education of children in a school environment. The School may pass information to other regulatory authorities where appropriate;
- Staff employment, including contract information (such as start date, hours worked, post, roles and salary information), work absence information (such as number of absences and reasons), payroll information (including bank account details) and special category personal data (such as medical information and ethnic group);
- The School may use names and photographs of staff in publicity and promotional material;
- To give a confidential reference relating to a staff member before or after resignation, for the purposes of their taking up employment elsewhere;
- For the purposes of management planning and forecasting, research and statistical analysis, including that imposed or provided for by law.

6.4. Staff should note that information about disciplinary action or safeguarding matters (as per the School's Safer Recruitment Policy) may be kept for longer than the duration of the sanction. Although treated as "spent" once the period of the sanction has expired, the details of the incident may need to be kept for a longer period.

Other Individuals

6.5. The School may hold personal information in relation to other individuals who have contact with the School, such as volunteers and guests. Such information shall be held only in accordance with the data protection principles, and shall not be kept longer than necessary.

7. Types of personal data

By way of example the types of personal data processed by the School include:

- names, addresses, date of birth, telephone numbers, e-mail addresses and other contact details;
- bank details and other financial information, e.g. about parents who pay fees to the school and staff payroll information;
- past, present and prospective pupils' academic, disciplinary, admissions and attendance records, including information about any special needs, and examination scripts and marks;
- logs of concerns, bullying and complaints, as required by the Independent School Standards Regulations;
- staff details including employment history, absence records, disciplinary and grievance records, performance review, training details, information relating to career progression, photographs, maternity and paternity and adoption leave;
- where appropriate, information about individuals' health, and contact details for their next of kin;
- references given or received by the school about pupils or staff, and information provided by previous educational or employment establishments and/or other professionals or organisations working with pupils or staff;
- photographs, videos, recordings and other images
- images captured by the school's CCTV system in accordance are used in accordance with the Information Commissioner’s Office (ICO) Code of Practice and the School's policy on taking, storing and using images of children;

8. Lawful basis for use of information

8.1. The School's primary condition for use of personal data is made in accordance with the School's legitimate interests, or the legitimate interests of another, provided that these are not outweighed by the impact on individuals.

8.2. In addition the School's processing is lawful because:

- The processing is necessary for the performance of an employment contract;
- The processing is necessary for the performance of a legal obligation to which the School is subject, for example our legal duty to safeguard pupils;
- The processing is necessary to protect the vital interests of others, i.e. to protect pupils from harm;
- The processing is necessary for the performance of the School's education function which is a function in the public interest.

8.3. The School will not usually need consent to use information apart from as detailed in the School's Taking, Storing and Using Images Policy and the School's Privacy Notices. However, if at any time the School will use personal data in a way which means consent is required this will be requested. If an individual gives their consent, they may change their mind at any time.

8.4. When the School collects personal information it will be made clear whether there is a legal requirement to provide it, and whether there is a legal requirement on the School to collect it. If there is no legal requirement then the School will explain why it is needed and what the consequences are if it is not provided.

8.5. If at any time the School wishes to use personal data in a way that requires an individual's consent, this will be explained to any individuals concerned and positive opt in consent will be requested. Individuals always have the right to withdraw consent, where given, or otherwise object to direct marketing or fundraising. However, the School may need nonetheless to retain some details, not least to ensure that no more communications are sent to that particular address, email or telephone number.

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 contact details of the controller (the school), and where applicable the controller's representative.

- 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 and the safeguards in place.
- 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.

8.4. 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 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. A subject access request must be made in writing. The School may ask for any further information reasonably required to locate the information.

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 undue 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.

9.12 Access to records will be refused in instances where an exemption applies, for example, information sharing may place the individual at risk of significant harm or jeopardise police investigations into any alleged offence(s).

9.13 An individual only has the automatic right to access information about themselves, and care needs to be taken not to disclose the personal data of third parties where consent has not been given, or where seeking consent would not be reasonable, and it would not be appropriate to release the information. Particular care must be taken in the case of any complaint or dispute to ensure confidentiality is protected.

9.14 Where all the data in a document cannot be disclosed a permanent copy should be made and the data redacted or retyped if this is more sensible. A copy of the full document and the altered document should be retained, with the reason why the document was altered.

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. The individual shall be given the option of a review under the Complaints Policy and Procedure, or an appeal direct to the Information Commissioner.

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 or objects to the processing and there is no other legal basis for 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.

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

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 Principal 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 individual dealing with the breach
- 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 drive and on a network drive that is regularly backed up 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 to hold personal information unless they are password-protected and fully encrypted.

18.6. All electronic devices are password-protected to protect the information on the device in case of theft.

18.7. Where possible, the school enables electronic devices to allow the remote blocking or deletion of data in case of theft.

18.8. Staff will not use their personal laptops or computers to process personal data

18.9. All necessary members of staff are provided with their own secure login and password,

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, are reviewed annually. If an increased risk in vandalism/burglary/theft is identified, extra measures to secure data storage will be put in place.

18.17. Goodwyn takes its Data Protection duties under the GDPR seriously and any unauthorised disclosure may result in disciplinary action.

18.18. The school manager is responsible for continuity and recovery measures are in place to ensure the security of protected data.

19. Publication of information

19.1. Goodwyn will not publish any personal information, including photos, on its website without the permission of the affected individual.

19.2. 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. CCTV and 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 notifies all pupils, staff and visitors of the purpose for collecting CCTV images via notice boards, letters and email.

20.3. Cameras are only placed where they do not intrude on anyone's privacy and are necessary to fulfil their purpose.

20.4. All CCTV footage will be kept for 14 days for security purposes;

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

20.6. 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.

20.7. Precautions, are taken when publishing photographs of pupils, in print, video or on the school website.

20.8. Images captured by individuals for recreational/personal purposes, and videos made by parents for family use, are exempt from the GDPR.

21. Data retention

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 or pulped, 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.

23. Policy review

23.1. This policy is reviewed every two years the Senior Leadership Team.

Written by:	**SLT**
Date:	**May 2020**
Review Date:	**May 2022**