DATA PROTECTION POLICY

Contents

Statement of intent

Statement of intent

Giles Academy (the school) is required to fulfil requirements under the General Data Protection (GDPR) which came into force on 25th May 2018 in how it collects, retains and disposes of certain information about its personnel members, governors and pupils.

The school may be required in certain circumstances to share certain information about its staff or pupils with other organisations, including but not exclusively to; other schools or educational establishments, local authorities (including potentially the social services department of such) educational bodies, Government Departments, health care providers of law enforcement agencies.

This policy is designed to ensure that all staff and governors are aware of their responsibilities and how the school complies with the core principles of GDPR.

Organisational methods of ensuring data is retained securely are imperative **Giles Academy** is committed to ensuring good practice to keep clear practical policies supported by written procedures.

Signed

…….. **Dated……..**

Headteacher

……. **Dated……**

Chair of Governors

1. Legal framework

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

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

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.'
- H M Government Handling of DBS Certificate Information.

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

- Complaints Policy
- IT Policy
- Freedom of Information Policy
- CCTV Policy
- GDPR Policy as applicable to public examinations (See appendix A to this policy.)
- Student Acceptable Use of ICT Policy

2. Applicable Data

2.1 For the purposes of this policy, **personal data** refers to information that relates to an identifiable, living, individual, including information such

as an online identifier, such as 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, for example 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 concerning health matters.

3. Principles

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

- In relation to individuals, processed lawfully, fairly and in a transparent manner.
- 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 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 is 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 the data subjects for no longer than is necessary for the purposes for which the personal data is processed; personal data may be stored for longer periods, in so far 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 methods

- Kept in a form, which permit required by the GDPR in order to safeguard the rights and freedoms of individuals.
- Processed in a manner that ensures appropriate security of 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 **Giles Academy** will implement appropriate technical and organisational measures to demonstrate that data is processed in line with the principles of GDPR.

4.2 The school will provide comprehensive, clear and transparent 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, 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 has been appointed in order to:

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

5.2 Mr. Stephen N. Robinson has been appointed by the school as DPO, provided that his duties as such do not lead to a conflict of interests.

5.3 Mr. Stephen N. Robinson is committed to acquiring professional knowledge and experience in data protection law, particularly that in relation to schools and to pass such knowledge and experience to the school's personnel and governors as appropriate.

5.4 The DPO will from time to time as appropriate report to the highest level of management at the school, being, Headteacher, the Board of Governors and its members.

5.5 The DPO will act independently and will not be penalised for performing his task.

5.6 Enough resources will be provided to enable the DPO to enable him to meet his 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 GDPR, data will be lawfully processed under the following conditions:

The consent of the data subject has been obtained and recorded as such.

Processing is necessary for:

- Compliance with 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 act 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.

6.3 Sensitive data will only be processed in 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 only relates to members or former members (or 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 data subject.
- Processing is necessary for:

    - Carrying out obligations under employment, social security or social protection law, or 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.
    - Courts are acting in their judicial capacity.
    - Reasons of substantial public interest or based on 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 based on 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 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 GDPR. Where the standard of consent cannot be met, an alternative legal basis for processing data must be found or processing must cease.
7.5 Consent accepted under the DPA will be reviewed to ensure it meets with the standards of GDPR; however, acceptable consent obtained under the DPA will not be re-obtained.
7.6 Consent can be withdrawn by the individual at any time.
7.7 The consent of the parents will be sought prior to processing of a child's 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 about the processing of their personal date 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 and the safeguards in place.
- The retention period of criteria used to determine the retention period.
- The existence of 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 consequences.

8.4 Where data is obtained directly from the data subject, information regarding the provision of personal data is part of a statutory or contractual requirement and the details of the categories of personnel data 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 source 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 addition 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 date in order to verify the lawfulness of the processing.

9.3 The school will verify the identity if 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 or where it is considered multiple requests are being made or are vexatious.

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 made 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 request 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 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 made 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 the right to complain to the supervisory authority and to a judicial remedy, within one month of the refusal.

9.11 If 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 date 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 supplied to.

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

10.5 Where an 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 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 in 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 or services to a child.

11.3 The school has the right to refuse a request for erasure where 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 claim

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 a 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 supress the school's processing of personal data.

12.2 In the even 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 the 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 rectification 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 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 removed, 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 Giles Academy 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 of the request being made.

13.10 Where the request is complex, or several requests have been received, the timeframe can be extended by two months, ensuring that the individual is informed of the extension and the reasoning for it within one month of the receipt of the request

13.11 Where no action is 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 is 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 to 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 firm any other information.

14.2 Individuals have the right to object to the following:

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

14.3 Where personal data is processed for the performance of a legal task or legitimate interest:

- In individual's ground for objecting must relate to his or her's 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 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 which 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 situation in order to exercise their right to object
- Where the process 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,

15 Privacy by design and privacy impact assessment

15.1 A school acting 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.

15.2 Data Protection Impact Assessments (DPIA'S) will be used to identify the most effective method of complying with the school's data protection obligations and meeting individual's expectations of privacy.

15.3 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 **Giles Academy's** reputation which might otherwise occur.

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

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

15.6 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.

15.7 The school will ensure that all DPIAs include the following information:

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

15.8 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.

16 Data Breaches

16.1 The term (personal data breach) refers to a breach of security which has led to destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

16.2 The head teacher will ensure that all staff members are made aware of, and understand, what constitutes as a data breach as part of their continuous development training.

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

16.4 All notifiable breaches will be reported to the relevant supervisory authority (Information Commissioner's Office ICO) within seventy-two hours of the school becoming aware of it.

16.5 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.

16.6 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 directly.

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

16.8 In the event of a breach sufficiently serious, the public will be notified without undue delay.

16.9 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 or public need to be notified.

16.10

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.

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

17. Data security

17.1 Confidential paper records will be kept in locked filing cabinets, drawers or safe with restricted access.

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

17.3 Digital data is coded, encrypted -site or password protected, both on a local hard drive and on a network drive that is regularly backed up off-site.

17.4 Where data is saved on removable storage or portable device, the device will be kept in a locked filing cabinet, drawer or safe when not in use.

17.5 Memory sticks will not be used to hold personal information unless they are password protected and fully encrypted.

17.6 All school owned electronic devices are password protected to protect the information on the device in case of theft.

17.8 Staff or governors will not use their personal laptops or computers for school purposes, unless they are password protected. They must not be left unattended where data is displayed or accessible by others not entitled to it.

17.9 All necessary members of staff are provided with their own secure login and password and every computer regularly prompts users to change their password.

17.10 Emails containing sensitive or confidential information are password protected if there are unsecure servers between the sender and the recipients.

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

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

17.13 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, for example devices under lock and key. The person taking the information from the school premises accepts full responsibility for the security of the data.

17.14 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, which has been outlined in a privacy notice.

17.15 Under no circumstances are visitors allowed access to confidential or personal information. Visitors to areas of the school containing sensitive information must and are supervised at all times.

17.16 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/trespass/theft is identified, extra measures to secure data storage will be put in place.

17.17 **Giles Academy** takes its duties under GDPR seriously and any unauthorised disclosure may result in disciplinary action.

17.18 **The Data Protection Officer** is responsible continuity and recovery measures are in place to ensure the security of personal data.

18. Publication of information

18.1 **Giles Academy** publishes a publication scheme on its website outlining classes of information that will be made routinely available, including:-

- Policies and procedures
- Annual reports
- Financial information

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

18.3 **Giles Academy** will not publish any personal information, including photos on its website without the permission of the affected individual.

18.4 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.

19 CCTV and photography

The school understands that recording images of identifiable individuals constitutes as processing personal information, so it is done in accordance with data protection principles.

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

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

19.4 All CCTV footage will be retained for eighteen days for security purposes before it is overwritten, unless required for further processing, for instance evidence retention, in which cases it is kept for six months or for such period as it is required for legitimate processing; the Data Protection Officer is responsible for ensuring the records are secure and allowing access.

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

19.6 If the school wishes to use images/video footage of pupils in a publication, such as the school website, social media, prospectus, or recordings of schools plays, concerts etc. written permission will be sought for the specified usage from the parent/guardian of the pupil.

19.7 Special care is taken to ensure that any image of a pupil is not disclosed or published if the school is prohibited from so doing by Court Order. Any such Court Order served on the school is retained with the pupil's school record and protected in the same form as all pupil data for such duration as is necessary under the terms of the Order and its terms (limited to matters of relevance) be disclosed to any subsisting members of the Senior Leadership Team.

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

20. Data retention

20.1 Data will not be kept for longer than is necessary in line with the school's Recorded Management Policy.

20.2 Unrequired data will be deleted as soon as practicable

20.3 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.

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

21. DBS data

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

(See HM Government Guidance on the Handling of DBS Certificate information.)

21.2 Data provided by the DBS will never be duplicated.

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

22. Policy review

22.1 This policy is reviewed every two years by the Data Protection Officer and the Headteacher.

The next scheduled review of this policy is **April 2021.**