GESHER SCHOOL

ENGAGE EMPOWER EDUCATE

Data Protection Policy

Date	Review Date	Data Protection Officer	Data Privacy Officer
March 2021	March 2022	Judicium Consulting Limited	Dafna Hyman

Contents

1. Aims

Gesher collects and uses personal information about staff, pupils, parents and other individuals who come into contact with Gesher School or the Gesher Trust. This information is gathered in order to enable it to provide education and other associated functions. All data is collected, stored and processed in accordance with the General Data Protection Regulation (GDPR) now referred to as the GDPR (UK) following Brexit and the provisions of the Data Protection Act 2018 (DPA 2018).

This policy applies to all personal data, regardless of whether it is in paper or electronic format and includes (but is not limited to):

Personal Information Relating to School Personnel

- contact details
- National Insurance numbers
- ethnic group
- employment contracts
- remuneration details
- qualifications
- absence information
- other relevant data relevant to Employees/Staff and Governors

Personal Information Relating to Pupils

- contact details
- national curriculum assessment results
- other assessment information
- attendance information
- any exclusion information
- transferring school
- ethnic group

- any special needs
    - therapist's reports
    - other professional reports
- relevant medical information
- accident reports
- incident reports
- other relevant data relevant to pupils' on-going education and welfare needs
- photographic and CCTV images

2. Policy Statement

The General Data Protection Regulation (GDPR) ensures a balance between an individual's rights to privacy and the lawful processing of personal data undertaken by organisations in the course of their business. It aims to protect the rights of individuals about whom data is obtained, stored, processed or supplied and requires that organisations take appropriate security measures against unauthorised access, alteration, disclosure or destruction of personal data.

The School will protect and maintain a balance between data protection rights in accordance with the GDPR. This policy sets out how we handle the personal data of our pupils, parents, suppliers, employees, workers and other third parties.

This policy does not form part of any individual's terms and conditions of employment with the School and is not intended to have contractual effect. Changes to data protection legislation will be monitored and further amendments may be required to this policy in order to remain compliant with legal obligations.

All members of staff are required to familiarise themselves with its content and comply with the provisions contained in it. Breach of this policy will be treated as a disciplinary offence which may result in disciplinary action under the School's Disciplinary Policy and Procedure up to and including summary dismissal depending on the seriousness of the breach.

No third party shall be permitted to access any Gesher personal data without first confirming in writing that they have read, understood and will comply fully with this policy and any other relevant data-related policies.

3. Legislation and Guidance

This policy meets the requirements of the GDPR and the expected provisions of the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the **GDPR** and the ICO's **code of practice for subject access requests**.

It also reflects the ICO's **code of practice** for the use of surveillance cameras and personal information.

4. Definitions

Term	Definition
Personal data	Any information relating to an identified, or identifiable, individual. This may include the individual's: • Name (including initials) • Identification number • Location data • Online identifier, such as a username It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.
Special categories of personal data	Personal data which is more sensitive and so needs more protection, including information about an individual's: • Racial or ethnic origin • Political opinions • Religious or philosophical beliefs • Trade union membership • Genetics • Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes • Health – physical or mental • Sex life or sexual orientation
Processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.
Data subject	The identified or identifiable individual whose personal data is held or processed.
Data controller	A person or organisation that determines the purposes and the means of processing of personal data.

Data processor	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

5. The Data Controller

Gesher School and the Gesher Trust are joint data controllers and data processors under the GDPR. Our school processes personal data relating to parents, pupils, staff, governors, visitors and others, and therefore is a data controller.

The school is registered as a data controller with the ICO and will renew this registration annually or as otherwise legally required. Details of the Trust's registration can be found on the ICO website.

6. Roles and Responsibilities

This policy applies to all our staff and governors, and to external organisations or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action.

6.1 Governing board

The governing board has overall responsibility for ensuring that our school complies with all relevant data protection obligations and has appointed a Data Protection Officer (DPO) who reports to the governing body and works with the Data Privacy Officer, who is a member of staff. The Headteacher and the Data Privacy Officer have responsibility for developing and encouraging good information handling practices within Gesher School.

6.2 Data protection officer

The data protection officer (DPO) is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies, procedures and guidelines where applicable.

The DPO is accountable to the Chair of Governors for the management of personal data within Gesher School and the Gesher Trust for ensuring that compliance with data protection legislation and good practice can be demonstrated.

The DPO is also the first point of contact for individuals whose data the school processes, and for the ICO.

Our DPO is contactable via email dpo@gesherschool.com

6.3 Data privacy officer

The Data Privacy Officer acts as the representative of the data controller on a day-to-day basis and can be contacted via the Gesher School office.

6.4 All staff

Compliance with data protection legislation is the responsibility of all Employees, Staff, Governors and Trustees of Gesher School and the Gesher Trust who process personal data. Staff are responsible for:

- collecting, storing and processing any personal data in accordance with this policy
- informing the school of any changes to their personal data, such as a change of address
- contacting the DPO in the following circumstances:
    - With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
    - If they have any concerns that this policy is not being followed
    - If they are unsure whether or not they have a lawful basis to use personal data in a particular way
    - If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the European Economic Area
    - If there has been a data breach
    - Whenever they are engaging in a new activity that may affect the privacy rights of individuals
    - If they need help with any contracts or sharing personal data with third parties

7. Data Protection Principles

All processing of personal data must be conducted in accordance with the data protection principles as set out in Article 5 of the GDPR. Gesher's policies and procedures are designed to ensure compliance with the principles.

The principles say that personal data must be:

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed
- Accurate and, where necessary, kept up to date
- Kept for no longer than is necessary for the purposes for which it is processed

- Processed in a way that ensures it is appropriately secure

This policy sets out how the school aims to comply with these principles.

8. Collecting Personal Data

8.1 Lawfulness, fairness and transparency

We will only process personal data where we have one of 6 'lawful bases' (legal reasons) to do so under data protection law:

- The data needs to be processed so that the school can **fulfil a contract** with the individual, or the individual has asked the school to take specific steps before entering into a contract
- The data needs to be processed so that the school can **comply with a legal obligation**
- The data needs to be processed to ensure the **vital interests** of the individual e.g. to protect someone's life
- The data needs to be processed so that the school, as a public authority, can perform a task **in the public interest,** and carry out its official functions
- The data needs to be processed for the **legitimate interests** of the school or a third party (provided the individual's rights and freedoms are not overridden)
- The individual (or their parent/carer when appropriate in the case of a pupil) has freely given clear **consent**

For special categories of personal data, we will also meet one of the special category conditions for processing which are set out in the GDPR and Data Protection Act 2018.

Gesher School's Privacy Notices are published on the Gesher School Website and are available from the School Office on request. Contact details of the DPO are published on our Privacy Notices.

The Data Protection Officer is responsible for ensuring that Gesher does not collect information that is not strictly necessary for the purpose for which it is obtained.

The Data Protection Officer, alongside the Data Privacy Officer, will ensure that - on an annual basis - all data collection methods are reviewed to ensure that collected data continues to be adequate, relevant and not excessive.

8.2 Limitation, minimisation and accuracy

We will only collect personal data for specified, explicit and legitimate reasons. We will explain these reasons to the individuals when we first collect their data.

If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so and seek consent where necessary.

8.21 Staff must only process personal data where it is necessary in order to do their jobs.

8.22 When staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with the school's Record Retention Schedule.

8.23 Data that is stored by the data controller is reviewed and updated as necessary. No data is kept unless it is reasonable to assume that it is accurate.

8.24 The Data Protection Officer is responsible for ensuring that all Staff, Governors and Trustees are trained in the importance of collecting accurate data and maintaining it.

8.25 On at least an annual basis, the Data Protection Officer, alongside the Data Privacy Officer, will review the retention dates of all the personal data processed by Gesher, by reference to the data inventory, and will identify any data that is no longer required in the context of the registered purpose. This data will be securely deleted/destroyed in line with the Secure Disposal of Storage Media Procedure (see Appendix 5).

8.26 The Data Protection Officer, alongside the Data Privacy Officer, is responsible for responding to requests for rectification from data subjects within one month as per the Subject Access Request Procedure (see Appendix 6). This can be extended to a further two months for complex requests. If Gesher decides not to comply with the request, the Data Protection Officer must respond to the data subject to explain its reasoning and inform them of their right to complain to the supervisory authority and seek judicial remedy.

8.27 The Data Protection Officer, alongside the Data Privacy Officer, is responsible for making appropriate arrangements that, where third-party organisations may have been passed inaccurate or out-of-date personal data, to inform them that the information is inaccurate and/or out of date and is not to be used to inform decisions about the individuals concerned; and for passing any correction to the personal data to the third party where this is required.

8.28 Where personal data is retained beyond the processing date, it will be pseudonymised in order to protect the identity of the data subject in the event of a data breach.

8.29 Personal data will be retained in line with the Retention and Disposal of Records Procedure (see Appendix 4) and, once its retention date is passed, it is securely destroyed as set out in this procedure.

8.210 The Data Protection Officer specifically approves any data retention that exceeds the retention periods defined in Retention of Records Procedure and ensures that the justification is clearly identified and in line with the requirements of the data protection legislation.

8.211 Gesher will demonstrate compliance with the data protection principles by implementing data protection policies, adhering to codes of conduct, implementing technical and organisational measures, as well as adopting techniques such as data protection by design, DPIAs, breach notification procedures and incident response plans.

9. Sharing Personal Data

We will not normally share personal data with anyone else, but may do so where:

- There is an issue with a pupil or parent/carer that puts the safety of our staff at risk
- There is an issue with the health, welfare or safeguarding of a pupil or employee
- We need to liaise with other agencies – we will seek consent as necessary before doing this
- Our suppliers or contractors need data to enable us to provide services to our staff and pupils. When doing this, we will:
    - Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law
    - Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us

We will also share personal data with law enforcement and government bodies where we are legally required to do so, including for:

- The prevention or detection of crime and/or fraud
- The apprehension or prosecution of offenders
- The assessment or collection of tax owed to HMRC
- In connection with legal proceedings
- Where the disclosure is required to satisfy our safeguarding obligations
- Research and statistical purposes, as long as personal data is sufficiently anonymised or consent has been provided

We may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of our pupils or staff.

Where we transfer personal data to a country or territory outside the European Economic Area, we will do so in accordance with current data protection law.

10. Data Transfers

All exports of data from within the European Economic Area (EEA) to non-European Economic Area countries (referred to in the GDPR as 'third countries') are) unlawful unless there is an appropriate "level of protection for the fundamental rights of the data subjects" (at the time of publishing this policy).

The transfer of personal data outside of the EEA is (currently) prohibited unless one or more of the specified safeguards, or exceptions, apply:

10.1 An adequacy decision

10.2 The European Commission can and does assess third countries, a territory and/or specific sectors within third countries to assess whether there is an appropriate

level of protection for the rights and freedoms of natural persons. In these instances, no authorisation is required.

10.3 Countries that are members of the European Economic Area (EEA) but not of the EU are accepted as having met the conditions for an adequacy decision.

If Gesher wishes to transfer personal data from the EU to an organisation in the United States it will check that the organisation has appropriate measures to secure this data. An example is the implementation of standard contractual clauses, but a variety of other alternatives may fit depending on the purpose of sharing and processing.

11. Consent

11.1 Gesher understands 'consent' to mean that data has been explicitly and freely given, and a specific, informed and unambiguous indication of the data subject's wishes that, by statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her. The data subject can withdraw their consent at any time.

11.2 Gesher understands 'consent' to mean that the data subject has been fully informed of the intended processing and has signified their agreement, while in a fit state of mind to do so and without pressure being exerted upon them. Consent obtained under duress or on the basis of misleading information will not be a valid basis for processing.

11.3 There must be some active communication between the parties to demonstrate active consent. Consent cannot be inferred from non-response to a communication. The Controller must be able to demonstrate that consent was obtained for the processing operation.

11.4 Gesher understands that, for sensitive data, explicit written consent of data subjects must be obtained unless an alternative legitimate basis for processing exists.

11.5 In most instances, consent to process personal and sensitive data is obtained routinely by Gesher, using our standard consent documents.

11.6 If Gesher were to provide online services to children, parental or custodial authorisation would be obtained. This requirement applies to children under the age of 16 (unless the Member State has made provision for a lower age limit, which may be no lower than 13).

12. Subject Access Requests and Other Rights of Individuals

12.1 Subject access requests

Individuals have a right to make a subject access request (SAR) to gain access to personal information that the school holds about them. This includes:

- Confirmation that their personal data is being processed
- Access to a copy of the data
- The purposes of the data processing
- The categories of personal data concerned
- Who the data has been, or will be, shared with
- How long the data will be stored for, or if this isn't possible, the criteria used to determine this period
- The source of the data, if not the individual
- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual

Data subjects may make data access requests as described in Subject Access Request Procedure (see Appendix 9); this procedure also describes how Gesher will ensure that its response to the data access request complies with the requirements of the GDPR. Requests should be made via the Subject Access Request Form and include:

- Name of individual
- Correspondence address
- Contact number and email address
- Details of the information requested

If staff receive a subject access request, they must immediately forward it to the DPO.

12.2 Children and subject access requests

Personal data about a child belongs to that child, and not the child's parents or carers. For a parent or carer to make a subject access request with respect to their child, the child must either be unable to understand their rights and the implications of a subject access request or have given their consent.

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

12.3 Responding to subject access requests

When responding to requests, we:

- May ask the individual to provide 2 forms of identification
- May contact the individual via phone to confirm the request was made
- Will respond within 1 month of receipt of the request
- Will provide the information free of charge

- May tell the individual we will comply within 3 months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within 1 month, and explain why the extension is necessary

We will not disclose information if it:

- Might cause serious harm to the physical or mental health of the pupil or another individual
- Would reveal that the child is at risk of abuse, where the disclosure of that information would not be in the child's best interests
- Is contained in adoption or parental order records
- Is given to a court in proceedings concerning the child

If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee which takes into account administrative costs.

A request will be deemed to be unfounded or excessive if it is repetitive or asks for further copies of the same information.

When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO.

12.4 Other data protection rights of the individual

In addition to the right to make a subject access request (see above), and to receive information when we are collecting their data about how we use and process it (see section 7), individuals also have the right to:

- Withdraw their consent to processing at any time, only where consent applies
- Ask us to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Challenge processing which has been justified on the basis of public interest
- Request a copy of agreements under which their personal data is transferred outside of the European Economic Area
- Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them)
- Prevent processing that is likely to cause damage or distress
- Be notified of a data breach in certain circumstances
- Make a complaint to the ICO
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)

Individuals should submit any request to exercise these rights to the DPO. If staff receive such a request, they must immediately forward it to the DPO.

13. Parental Requests to See the Educational Record

Parents, or those with parental responsibility, have a legal right to free access to their child's educational record (which includes most information about a pupil). A response needs to be made within 15 school days of receipt of a written request.

14. CCTV

We use CCTV in various locations around the school site to ensure it remains safe. We, along with our security partners CST, adhere to the ICO's **code of practice** for the use of CCTV.

We do not need to ask individuals' permission to use CCTV, but we make it clear where individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is being used and directing enquiries about its use to **cctv@cst.org.uk**

15. Photographs and Videos

As part of our school activities and to outreach to parents and supports, we may take photographs and record images of individuals within our school.

We obtain consent from parents/carers for photographs and videos to be taken of their child for communication and promotional purposes. This may include within school on notice/display boards and in school newsletters and via our social media platforms.

Consent can be refused or withdrawn at any time. If consent is withdrawn, we remove the photograph or video and not distribute it further.

16. Data protection by Design and Default

We will put measures in place to show that we have integrated data protection into all of our data processing activities, including:

- Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge
- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law (see section 6)
- Completing data privacy impact assessments (DPIAs) where the school's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on this process)

- Integrating data protection into internal documents including this policy, any related policies and privacy notices
- Regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters
- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant
- Maintaining records of our processing activities, including:
    - For the benefit of data subjects, making available contact details of our school and DPO and all information we are required to share about how we use and process their personal data (via our privacy notices)
    - For all personal data that we hold, creating and maintaining an internal record of the type of data, data subject, how and why we are using the data, any third-party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure

17. Data Security and Storage of Records

All Employees/Staff/Governors and Trustees are responsible for ensuring that any personal data that Gesher holds and for which they are responsible, is kept securely and is not under any conditions disclosed to any third party unless that third party has been specifically authorised by Gesher to receive that information.

All personal data should be accessible only to those who need to use it, and access may only be granted in line with the Access Control Policy. All personal data is treated with the highest security, in particular:

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data are to be locked away when not in use and/or password protected
- Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, pinned to notice/display boards, or left anywhere else where there is general access. This is in accordance with our Clear Screen and Desk Policy
- Where personal information needs to be taken off site, staff must adhere to our Remote Working Policy
- If computerised, password protected in line with requirements in the Access Control Policy and/or stored on (removable) computer media which are encrypted in line with Secure Disposal of Media Procedure (see Appendix 5);
- Staff and pupils are not to share passwords
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices
- Staff, pupils or governors who remotely access personal information on their personal devices are expected to follow the same security and data protection

procedures as for school-owned equipment and in accordance with our Acceptable Use of IT policy and Remote Working Policy

- Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected (see section 8)

18. Disposal of Records

18.1 Gesher does not keep personal data in a form that permits identification of data subjects for longer a period than is necessary, in relation to the purpose(s) for which the data was originally collected.

18.2 Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it.

18.3 For example, we will securely dispose of paper-based records, and overwrite or delete electronic files. We may also use a third party to safely dispose of records on the school's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

18.4 When Gesher stores data for longer periods - if the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes – it is subject to the implementation of appropriate technical and organisational measures to safeguard the rights and freedoms of the data subject.

18.5 The retention period for each category of personal data will be set out in the Record Retention Schedule along with the criteria used to determine this period including any statutory obligations Gesher has to retain the data.

18.6 Personal data may only be deleted or disposed of in line with the Retention and Disposal of Records Procedure (see Appendix 4). Manual records that have reached their retention date are shredded and disposed of as 'confidential waste'. Hard drives of redundant PCs are to be removed and immediately destroyed before disposal.

19. Personal Data Breaches

The school will make all reasonable endeavours to ensure that there are no personal data breaches. In the unlikely event of a suspected data breach, we will follow the procedure set out in Appendix 3.

When appropriate, we will report the data breach to the ICO within 72 hours. Such breaches in a school context may include, but are not limited to:

- A non-anonymised dataset being published on the school website which shows the exam results of pupils eligible for the pupil premium

- Safeguarding information being made available to an unauthorised person
- The theft of a school laptop containing non-encrypted personal data about pupils

20. Training

All staff and governors are provided with data protection training as part of their induction process. Data protection will also form part of continuing professional development, where changes to legislation, guidance or the school's processes make it necessary.

21. Links with other policies

This data protection policy is linked to our:

- Access Control Policy
- Clear Screen and Desk Policy
- GDPR Training Policy
- Privacy notices
- Remote working policy
- Record Retention Schedule

22. Monitoring arrangements

The DPO is responsible for monitoring and reviewing this policy.

A current version of this document is published on the Gesher website.

This policy will be reviewed and updated if necessary. Otherwise, or from then on, this policy will be reviewed every year and shared with the full governing board.

Appendix 1: Data Consent Procedure

1. Scope

1.1 The consent of the data subject is one of the conditions for the processing of his or her personal data and is within the scope of this procedure. Gesher School and/or the Gesher Trust need to obtain consent when no other lawful basis applies.
1.2 Consent of the data subject is defined by the GDPR as "any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her".
1.3 Explicit consent is required for the processing of sensitive personal data. Specific conditions apply to the validity of consent given by children in relation to information society services, with requirements to obtain and verify parental consent below certain age limits.

2. Responsibilities

As a data controller, Gesher School and the Gesher Trust are responsible under the GDPR for obtaining consent from the data subject under advisement from the Data Protection Officer.

3. Consent procedure

3.1 Gesher provides clear privacy notices wherever personal data is collected to ensure that consent is informed and that the data subject is informed of their rights in relation to their personal data.
3.2 Gesher obtains data subject(s) consent to the processing of his or her personal data in the case explicit consent for sensitive personal data.
3.3 Gesher obtains data subject(s) consent to the processing of his or her personal data for one or more specific purposes.
3.4 Gesher demonstrates data subject(s) consent is clearly distinguishable from any other matter relating to the data subject (if recorded in paper / electronic file format use).
3.5 Gesher demonstrates data subject(s) consent is intelligible and accessible using clear and plain language.
3.6 Gesher demonstrates processing of data is limited to that stated in the contract and bound by the explicit consent given by the data subject.

4. Child consent procedure

4.1 Where processing relates to a child under 16 years old, Gesher demonstrates that consent has been provided by the person who is the holder of parental responsibility over the child, in instances where Gesher process data related to a child or children.

4.2 Gesher demonstrates reasonable efforts have been made to verify the age of the child and establish the authenticity of the parental responsibility.

Appendix 2: Data Protection Impact Assessment (DPIA) Procedure

1. Scope

1.1 All projects that involve processing personal data, or any activities (both internal and external) that affect the processing of personal data and impact the privacy of data subjects are within the scope of this procedure and will be subject to a data protection impact assessment (DPIA).

2. Responsibilities

2.1 The Data Protection Officer is responsible for performing necessary checks on personal data to establish the need for conducting a DPIA.

2.2 The Headteacher, The Data Privacy Officer and Data Protection Officer are responsible for checking appropriate controls are implemented to mitigate any risks identified as part of the DPIA process and subsequent decision to proceed with the processing.

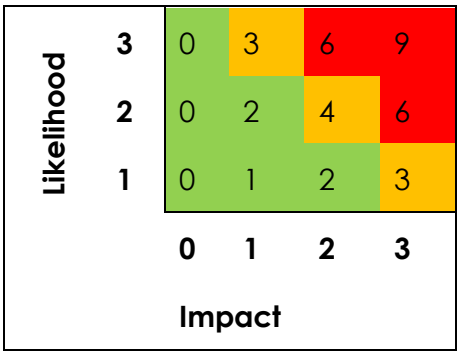
2.3 The Headteacher is responsible for implementing any privacy risk solutions identified.

3. Procedure

3.1 The Data Protection Officer, The Data Privacy Officer or Headteacher identifies the need for a DPIA, assessing the project and type of personal data involved, or processing activity.

3.2 Using the criteria below, following the likelihood and impact matrix, Gesher defines the risks to rights and freedoms of data subjects.

Likelihood and impact matrix:



Risks to rights and freedoms of data subjects:

Risk Level	From	To	GDPR Assessment
High	6	9	Highest unacceptable risk
Medium	3	5	Unacceptable risk
Low	1	2	Acceptable risk
Zero	0	0	No risk

4. Data processing workbook

4.1 Gesher records key information about data subjects via a data mapping or audit exercise. This includes a description of the processing and purposes; legitimate interests pursued by the controller; an assessment of the necessity and proportionality of the processing; an assessment of the risks to the rights and freedoms of data subjects (as per the matrix and risk level definitions in clause 3.2 above).

4.2 Gesher captures the type of processing activity associated with the personal data being processed as part of the project in the data mapping or audit exercise. These are categorised as:

- Collection
- Transmission
- Storage
- Access
- Deletion

4.3 Gesher establishes on what lawful basis the data is being processed and its appropriate retention period (in line with Retention and Disposal of Records Procedure).

4.4 Gesher identifies the category of data processed, whether it is personal, special or that of a child's, and the format of the data.

4.5 Gesher identifies who has access to the data (individuals, teams, third-parties or data processor) or who are involved in the processing of personal data, or processing activity, recording the geographic location of where the processing takes place and / or if it is transborder processing.

5. Identify privacy risks

5.1 Gesher assesses the privacy risks for each process activity as described in clause 3 above by:

5.1.1 Identifying and describing the privacy risk associated to that process activity

5.1.2 Using the likelihood criteria (1 – low, 2 – medium and 3 - high), scoring the likelihood of the risk occurring

5.1.3 Using the impact criteria (0 – zero impact, 1 – low, 2 – medium and 3 - high) of the risk should it occur

5.1.4 Producing a calculated risk, identifying the risk to the rights and freedoms of data subjects.

5.2 In assessing the privacy risks, Gesher considers: risks to the rights and freedoms of natural persons resulting from the processing of personal data; risks to the business (including reputational damage); and its objectives and obligations (both regulatory and contractual).

5.3 Gesher identifies solutions to privacy risks, assigns a risk treatment owner and sets a target date for completion.

5.4 Gesher prioritises analysed risks for risk treatment based on the risk level criteria established in clause 3.2 above.

5.5 Gesher as risk owner, in consultation with its Data Protection Officer, approves and signs off each DPIA for each data processing activity.

6. Prior consultation (Article 36, GDPR)

6.1 Where the DPIA identifies that processing of personal data will result in high risk to the data subject, in the absence of risk mitigating measures and controls, Gesher consults with the Local Education Authority or other appropriate supervisory authority.

6.2 When Gesher requests consultation from a supervisory authority it provides the following information:

- 6.2.1 detail of the responsibilities of Gesher School and/or Gesher Trust (as controller/processor or joint controller), and the data controller/processor or joint controller] involved in the processing;
- 6.2.2 purpose of the intended processing;
- 6.2.3 detail of any/all measures and controls in place/provided to protect the rights and freedoms of the data subject(s);
- 6.2.4 contact details of the Data Protection Officer
- 6.2.5 a copy of the data protection impact assessment; and
- 6.2.6 any other information requested by the supervisory authority.

Appendix 3: Personal Data Breech Notification Procedure

1. Scope

1.2 This procedure applies in the event of a personal data breach under Article 33 of the GDPR – *Notification of a personal data breach to the supervisory authority* – and Article 34 – *Communication of a personal data breach to the data subject*.

1.3 The GDPR draws a distinction between a 'data controller' and a 'data processor' in order to recognise that not all organisations involved in the processing of personal data have the same degree of responsibility. Each organisation should establish whether it is data controller, or a data processor for the same data processing activity; or whether it is a joint controller.

2. Responsibility

2.1 All users (whether Employees/Staff/Governors/Trustees, contractors or temporary Employees/Staff and third party users) of Gesher School and Gesher Trust are required to be aware of, and to follow this procedure in the event of a personal data breach.

2.2 All Employees, Staff, Governors and Trustees, contractors or temporary personnel are responsible for reporting any personal data breach to the Data Protection Officer or Data Privacy Officer.

3. Procedure – Breach notification data processor to data controller

3.1 Gesher reports any personal data breach or security incident to the Data Protection Officer without undue delay. Gesher provides the DPO with all of the details of the breach.

3.2 The breach notification is made in writing or by email.

3.3 A confirmation of receipt of this information is made by email.

4. Procedure – Breach notification data controller to supervisory authority

4.1 The Data Protection Officer determines if the supervisory authority need to be notified in the event of a breach.

4.2 The Data Protection Officer assesses whether the personal data breach is likely to result in a risk to the rights and freedoms of the data subjects affected by the personal data breach, by conducting a data protection impact assessment (DPIA) against the breach.

4.3 If a risk to data subject(s) is likely, Gesher reports the personal data breach to the supervisory authority (typically the ICO) without undue delay, and not later than 72 hours.

4.4 If the data breach notification to the supervisory authority is not made within 72 hours, Gesher's Data Protection Officer submits it electronically with a justification for the delay.

4.5 If it is not possible to provide all of the necessary information at the same time Gesher will provide the information in phases without undue further delay.

4.6 The following information needs to be provided to the supervisory authority:

4.6.1 A description of the nature of the breach.

4.6.2 The categories of personal data affected.

4.6.3 Approximate number of data subjects affected.
4.6.4 Approximate number of personal data records affected.
4.6.5 Name and contact details of the Data Protection Officer.
4.6.6 Consequences of the breach.
4.6.7 Any measures taken to address the breach.
4.6.8 Any information relating to the data breach.

4.7 The Data Protection Officer notifies the supervisory authority (typically the ICO).
4.8 In the event the supervisory authority assigns a specific contact in relation to a breach, these details are recorded in the Internal Breach Register.
4.9 The breach notification is made by email.
4.10 A confirmation of receipt of this information is made by email.

5. Procedure – Breach notification data controller to data subject

5.1 If the personal data breach is likely to result in high risk to the rights and freedoms of the data subject, Gesher notifies those/the data subjects affected immediately.
5.2 The notification to the data subject describes the breach in clear and plain language, in addition to information specified in clause 4.6 above.
5.3 Gesher takes measures to render the personal data unusable to any person who is not authorised to access it using encryption.
5.4 The data controller takes subsequent measures to ensure that any risks to the rights and freedoms of the data subjects are no longer likely to occur.
5.5 If the breach affects a high volume of data subjects and personal data records, Gesher makes a decision based on assessment of the amount of effort involved in notifying each data subject individually, and whether it will hinder Gesher's ability to appropriately provide the notification within the specified time frame. In such a scenario a public communication or similar measure informs those affected in an equally effective manner.
5.6 If Gesher has not notified the data subject(s), and the supervisory authority considers the likelihood of a data breach will result in high risk, Gesher will communicate the data breach to the data subject.
5.7 Gesher documents any personal data breach(es), incorporating the facts relating to the personal data breach, its effects and the remedial action(s) taken.

Appendix 4: Retention and Disposal of Records Procedure

1. Scope

All Gesher School and Gesher Trust's records, whether analogue or digital, are subject to the retention requirements of this procedure.

2. Responsibilities

2.1 The following roles are responsible for retention and disposal of these records because they are the information asset owners.
2.2 Asset owners are/responsible for ensuring that all personal data is collected, retained and destroyed in line with the requirements of the GDPR.
2.3 The Chair of Governors is responsible for retention and disposal of financial (accounting, tax) and related records.
2.4 The Headteacher is responsible for retention and disposal of all HR records.
2.5 The Health and Safety Governor is responsible for retention and disposal of all Health and Safety records
2.6 The Headteacher is responsible for retention and disposal of all other statutory and regulatory records.
2.7 The Data Protection Officer is responsible for storage and disposal of data in line with this procedure.
2.8 The Headteacher is responsible for ensuring that retained records are included in any disaster recovery plans.

3. Procedure

3.1 The required retention periods, by record type, are recorded in (Retention of Records) under the following categories:
  3.1.1 Record type
  3.1.2 Retention period
  3.1.3 Retention period to start from (at creation, submission, payment, etc.)
  3.1.4 Retention justification
  3.1.5 Record medium
  3.1.6 Disposal method
3.2 Each data asset that is stored is to be added to the Data Registry and/or Data Audit and marked with the name of the record, the record type, the original owner of the data, the information classification, the data of storage, the required retention period, the planned date of destruction, and any special information.
3.3 For all storage media (electronic and hard copy records), Gesher retains the means to access that data, if and where appropriate, within the scope of current data protection law.
3.4 For all electronic storage media, Gesher does not exceed the manufacturer's recommended 90% storage life. When the maximum of 90% is reached, the stored data is copied onto new storage media and stored on the School's Domain controller which is located in the comms room. Access to the server room is restricted by a code entry system.
3.5 The Headteacher is responsible for managing the process of destroying data once it has reached the end of the retention period as specified in the Retention and Disposal Schedule. Secure destruction is completed within 30 days of the planned retention period.
3.6 Portable/removable storage media are destroyed in line with this policy.

Appendix 5: Secure Disposal of Media Procedure

1. Scope

Gesher requires that all removable storage media are clean (which means it is not possible to read or reconstitute the information that was stored on the device or document) prior to disposal.

2. Responsibilities

2.1 The Data Privacy Officer is responsible for managing the secure disposal of all storage media in line with this procedure when they are no longer required and is responsible for ensuring the removal of shredded documents.
2.2 All owners of removable storage media are responsible for ensuring that these media are disposed of in line with this procedure.

3. Procedure

3.1 Hard disks are cleared of all software and all organisational confidential and restricted information prior to disposal or reuse, as set out in Clause 3.5 and 3.6, below.
3.2 The Data Privacy Officer is responsible for the secure disposal of storage media and the disposal of all information processing equipment. A log is retained showing what media were destroyed and/or disposed of, and when. The information asset inventory and/or data inventory is adjusted once the asset has been disposed of.
3.3 When hard disks need to be cleaned this will be carried out by Delta Security and managed by IT services.
3.4 Devices containing confidential information, which cannot be removed, are destroyed prior to disposal and are never reused.
3.5 Devices containing confidential information that are damaged are subject to a risk assessment prior to sending for external repair, to establish whether they should be repaired or replaced.
3.6 Portable or removable storage media of any description are destroyed prior to disposal.
3.7 All media are disposed of through Gesher's approved contractor.
3.8 Documents containing confidential and restricted information are destroyed by using a shredder with an appropriate security classification. The shredder is located in the school office.

Appendix 6: Subject Access Request Procedure

1. Scope

All personal data processed by Gesher School and the Gesher Trust is within the scope of this procedure.

Data subjects (or parents/legal guardians of data subjects) are entitled to obtain:

- Confirmation as to whether Gesher School and/or the Gesher Trust is processing any personal data about that individual;
- Access to their personal data;
- Any related information.

2. Responsibilities

2.1 The Data Protection Officer is responsible for the application and effective working of this procedure, and for reporting to the information owner – the Headteacher or Data Privacy Officer - on Subject Access Requests (SARs).

2.2 The Data Protection Officer assisted by the Data Privacy Officer, is responsible for handling all SARs.

3. Procedure

3.1 Subject Access Requests are made using the Subject Access Request Form.

3.2 The data subject provides Gesher with evidence of their identity, in the form of a current passport/driving license, and the signature on the identity must be cross-checked to that on the application form.

3.3 The data subject specifies to Gesher specific set of data held by Gesher School and/or the Gesher Trust on their subject access request (SAR). The data subject can request all data held on them.

3.4 Gesher records the date that the identification checks were conducted and the specification of the data sought.

3.5 Gesher provides the requested information to the data subject within one month from this recorded date.

3.6 Once received, the subject access request (SAR) application is immediately forwarded to the Data Protection Officer, who will ensure that the requested data is collected within the specified time frame in clause 3.4 above.

Collection entails:

3.6.1 Collecting the data specified by the data subject, or

3.6.2 Searching all databases and all relevant filing systems (manual files), including all back up and archived files (computerised or manual) and all email folders and archives. The Data Privacy Officer maintains a data map or audit that identifies where all Gesher is stored.

3.7 The Data Privacy Officer maintains a record of requests for data and of its receipt, including dates.

3.8 The Data Protection Officer reviews subject access requests from a child. Before responding to a SAR of the child data subject the Data Protection Officer considers their ability to making the request.

3.9 The Data Protection Officer reviews all documents that have been provided to identify whether any third parties are present in it, and either removes the identifying

third party information from the documentation or obtains written consent from the third party for their identity to be revealed.

3.10 If any of the requested data is being held or processed under one of the following exemptions, it does not have to be provided:

- National security
- Crime and taxation
- Health
- Education
- Social Work
- Regulatory activity
- Journalism, literature and art
- Research history, and statistics
- Publicly available information
- Corporate finance
- Examination marks
- Examinations scripts
- Domestic processing
- Confidential references
- Judicial appointments, honours and dignities
- Crown of ministerial appointments
- Management forecasts
- Negotiations
- Legal advice and proceedings
- Self-incrimination
- Human fertilization and embryology
- Adoption records
- Special educational needs
- Parental records and reports

3.11 In the event that a data subject requests Gesher School and/or Gesher Trust to provide them with the personal data stored by the controller/processor, then Gesher will provide the data subject with the requested information in electronic format, unless otherwise specified.

3.12 In the event that a data subject requests what personal data is being processed then Gehser provides the data subject with the following information:

3.12.1 Purpose of the processing

3.12.2 Categories of personal data

3.12.3 Recipient(s) of the information, including recipients in third countries or international organisations

3.12.4 How long the personal data will be stored

3.12.5 The data subject's right to request rectification or erasure, restriction or objection, relative to their personal data being processed.

3.12.5.1 Gesher removes personal data from systems and processing operations as soon as a request for erasure has been submitted by the data subject.

3.12.5.2 Gesher takes appropriate measures without undue delay in the event that the data subject has: withdrawn consent; objects to the processing of their personal data in whole or part; no longer under legal obligation and/or has been unlawfully processed.

3.12.6 Inform the data subject of their right to lodge a complaint with the supervisory authority and a method to do so.

3.12.7 Information on the source of the personal data if it hasn't been collected from the data subject.

3.12.8 Inform the data subject of any automated decision-making.

3.12.9 If and where personal data has been transferred and information on any safeguards in place.

Appendix 7: Withdrawal of Consent Procedure

1. Scope

This procedure addresses the data subject(s) right to withdraw consent for the processing of his or her personal data.

Withdrawal of consent by the data subject means an unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies withdrawal of consent to the processing of personal data relating to him or her where consent applies as a legal basis.

2. Responsibilities

As a data controller, Gesher School and/or the Gesher Trust , is responsible under the GDPR for administering withdrawal of consent from the data subject under advisement from Data Protection Officer.

3. Withdrawal of consent procedure

3.1 Gesher demonstrates the data subject has withdrawn consent to the processing of his or her personal data as recorded in the Data Subject Consent Withdrawal form.

3.2 Where the processing had multiple purposes, Gesher demonstrates withdrawal of consent for each purpose as recorded in the Data Subject Consent Withdrawal form.

3.3 The processing activities that relied upon the consent is stopped in accordance with the relevant process. The Data Protection Officer will inform the relevant process owner of this change so that processing can be stopped.

3.4 Please note that where consent does not apply as a legal basis, Gesher will not accept a withdrawal of consent and continue to process personal data as per legal requirements based on the legitimate reason of processing.

4. Withdrawal of parental consent procedure

4.1 Gesher demonstrates the holder of parental responsibility over the specified child has withdrawn consent via the Parent Consent Withdrawal.

4.1 Gesher demonstrates that reasonable efforts have been made to establish the authenticity of the parental responsibility when withdrawing consent for the specified child.

4.1 The processing activities that relied upon the consent is stopped in accordance with the relevant process. The Data Protection Officer will inform the relevant process owner of this change so that processing can be stopped.

4.1 Please note that where consent does not apply as a legal basis, Gesher will not accept a withdrawal of consent and continue to process personal data as per legal requirements based on the legitimate reason of processing.