Aureus School Buildings
Candytuft Way
Harwell
Didcot
Oxon, OX11 6FF

Tel: 01235 313713
Email: info@questforlearning.org.uk
Website: www.questforlearning.org.uk

QfL Data Protection Policy

1. Aim

The aim of Quest for Learning (QfL), is to ensure all personal data collected about staff, pupils, parents, Trustees, volunteers and other individuals is stored and processed in accordance with the General Data Protection Regulation (GDPR) and the provisions set out in the Data Protection Act 2018 (DPA 2018).

This policy applies to all personal data, regardless of whether it is in paper or electronic format.

2. Legislation and Guidance

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

3. Definitions

Term	Definition
Consent	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.
Data subject	The identified or identifiable individual whose personal data is held or processed.
Data set	A group of identified able data subjects, such as pupils, staff, parents, etc.
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	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.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.
Suppression List	A register recording the details of data subjects that do not consent to specific information being sent, emailed or copied to them.

4. The Data Controller

QfL processes personal data relating to pupils, staff, trustees, visitors and others, and therefore is a data controller and is registered as a data controller with the ICO and renews this registration annually or as otherwise legally required.

5. Roles and Responsibilities

This policy applies to all staff employed by QfL and to external organisations or individuals working on its behalf. Staff who do not comply with this policy may face disciplinary action.

5.1 QfL Board of Trustees

The Board has overall responsibility for ensuring QfL fully complies with all relevant data protection obligations.

5.2 QfL Executive Director

The Executive Director acts as the representative of the Data Controller on a day-to-day basis.

5.3 Data Protection Officer (DPO)

The ICO does not require QfL to appoint a DPO, however QfL has a designated an employee (DE) who is responsible for data protection within the charity. The employee is responsible for overseeing the implementation of this policy, monitoring compliance with data protection law and developing related policies and guidelines where applicable. The designated employee is also the point of contact for individuals whose data QfL processes and for the ICO.

5.4 All staff

Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Informing the charity of any changes to their personal data, such as a change of address
- Contacting the QfL designated employee responsible for data protection:
    - 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

6. Data Protection Principles

GDPR is based on the following data protection principles and states 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 is 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 secured

This policy sets out how Quest for Learning aims to comply with these principles.

7. Collecting Personal Data

7.1 Lawfulness, fairness and transparency

QfL will only process personal data where there is a "lawful basis" (legal reasons) to do so under data protection law:

- The data needs to be processed so that QfL can **fulfil a contract** with the individual or organisation, or the individual has asked QfL to take specific steps before entering into a contract
- The data needs to be processed so that QfL 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**

QfL will not often need to use consent, however, where it is sought the following is to apply:

- individuals are to have a positive opt-in, the use of pre-ticked boxes or any other method of default consent is not to be used;
- it is to be clear, concise, specific and 'granular' i.e. separate consent is obtained for each request, vague or blanket consent is not sufficient;
- requests for consent are to be separate from other terms and conditions;
- where consent is collected and used by a third party, the third party is to be named;
- explicit consent (used for special category data) requires a very clear and specific statement;
- individuals are to be told they can withdraw their consent at any time, how to withdraw their consent (the withdrawal process is to be clear and easy);
- QfL is to keep evidence of consent i.e. who was asked, when were they asked, how they were asked (letter, software, etc.), what they were asked and what the rationale for their consent;
- consent is to be kept under review and refreshed if there are anything changes;
- consent is not to be a precondition of a service;

QfL will meet one of the special category conditions for processing set out in the GDPR and DPA 2018:

- the data subject has given explicit consent;
- processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law
- processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;
- processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects
- processing relates to personal data which are manifestly made public by the data subject;
- processing is necessary for the establishment, exercise or defence of legal claims;
- processing is necessary for reasons of substantial public interest;
- processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of law or pursuant to contract with a health professional;
- processing is necessary for reasons of public interest in the area of public health;

- processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.

7.2 Limitation, minimisation and accuracy

QfL will only collect personal data for specified, explicit and legitimate reasons and will explain these reasons to individuals when the information is first gathered i.e. via a Privacy Notice.

Should QfL want to use personal data for reasons other than those provided when the data was first obtained it will inform the individuals concerned before doing so and, where necessary, seek consent.

Staff must only process personal data where it is necessary in order carry out their job. When staff no longer need the personal data they hold, they must ensure it is deleted or anonymised and this should be undertaken in accordance with QfL's Records Retention Schedule.

8. Sharing Personal Data

QfL will not normally share personal data, but may do so where:

- There is an issue with a pupil or parent/carer that puts the safety of our staff at risk
- QfL needs to liaise with other agencies – we will seek consent as necessary before doing this
- Suppliers or contractors need data to enable QfL to provide services to staff and pupils – for example, housing associations, IT providers. When doing this, QfL will:
    - Only appoint suppliers or contractors that can provide sufficient guarantees they comply with data protection law
    - Establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of the shared personal data
    - Only share data and information that the supplier or contractor needs to carry out their service and to keep them safe while working with QfL

QfL will also share personal data with law enforcement and government bodies where 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 safeguarding obligations
- Research and statistical purposes, as long as personal data is sufficiently anonymised, or consent has been provided

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

Where personal data is transferred to a country or territory outside the European Economic Area, it will do so in accordance with data protection law.

9. Subject Access Requests and Other Rights of Individuals

9.1 Subject Access Requests

Individuals have a right to make a 'subject access request' to gain access to personal information held about them. This includes:

- Confirmation 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

Subject access requests must be submitted using the appropriate request form, either by letter or email to: The Administrator, Quest for Learning, Aureus School Building, Candytuft Way, Harwell, Didcot, Oxfordshire, OX11 6FF, 01235 313713, info@questforlearning.org.uk

9.2 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 13** 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 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.

Children **aged 13 and older** are generally 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 may not be granted without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

9.3 Responding to Subject Access Requests

When responding to requests QfL will:

- Ask individuals to prove their identification
- Contact the individual via phone to confirm the request was made
- Respond without delay and within 1 month of receipt of the request
- Provide the information free of charge
- Inform and explain to individuals, where a request is complex or numerous, that the charity requires an extension to the time limit and the information will be provided within 3 months from the original date of the request

QfL will not disclose information if it:

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

If the request is unfounded or excessive, QfL may refuse to act on it, or charge a reasonable fee taking 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 refusing a request, QfL will inform individuals why and they have the right to complain to the ICO.

9.4 Other Data Protection Rights of the Individual

In addition to the right to make a subject access request, and to receive information when collecting data, individuals also have the right to:

- At any time, withdraw their consent to processing
- Ask QfL to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances)
- Prevent the use of their personal data for direct marketing
- Challenge processing, which has been justified based on "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 a request to exercise these rights, using the relevant request form, either by letter or email to: The Administrator, Quest for Learning, Aureus School Building, Candytuft Way, Harwell, Didcot, Oxfordshire, OX11 6FF, 01235 313713, info@questforlearning.org.uk

10. Data Protection by Design and Default

QfL has measures in place to demonstrate that data protection has been integrated into data processing activities, including:

- The appointment of a designated employee responsible for data protection, and ensuring he/she has 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
- Completing privacy impact assessments where the processing of personal data presents a high risk to the rights and freedoms of individuals and when introducing new technologies
- Integrating data protection into internal documents and related policies and privacy notices
- Regularly training members of staff on data protection law, this policy, any related policies, any other data protection matters and record attendance to training
- Regularly conducting reviews and audits to test privacy measures and check compliance
- Maintaining records of our processing activities, including:
    - For the benefit of data subjects, making available the name and contact details of the DE
    - The use of Privacy Notices to inform all data sets about the information held, how it is used and if it is shared, with whom
    - Maintaining an internal record of the type of data QfL collects, how it uses it, the relevance of the data to the data sets, where the data is stored and the retention period for the data

11. Data Security and Storage of Records

QfL will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure and against accidental or unlawful loss, destruction or damage. In particular:

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data are kept secured when not in use.

- Papers containing confidential personal data are not left on office desks, pinned to notice/display boards or left anywhere else where there is general access.
- Where homeworking is required staff adhere to guidelines set out in the QfL Homeworking Guidelines.
- Complex (secure) passwords are used to secure all data files and email files.
- Portable devices, such as USB sticks or external hard drives, will only be used when there is no alternative. These devices will be fully encrypted before being used to store QfL data.
- Where personal data is shared with a third party, QfL undertakes due diligence and reasonable steps to ensure it is stored securely and is adequately protected

12. Disposal of Records

Personal data that is no longer needed, is inaccurate or out of date and cannot or does not need to be rectified is to be disposed of securely.

QfL will shred or incinerate paper-based records and overwrite or delete electronic files. If using third party organisations to safely dispose of records, QfL will obtain sufficient guarantees from the supplier to satisfy themselves that they are complying with data protection law.

Before disposing of documents staff are to check the QfL Records Retention Schedule to confirm retention dates.

13. Data Breaches

QfL will make all reasonable endeavours to ensure personal data is protected and there are no data breaches. When appropriate, the Charity will report the data breach to the ICO within 72 hours. Data breach procedures are detailed in *Annex A.*

14. Training

All Trustees, governors and staff are provided with data protection training as part of their induction process.

Where changes to legislation, guidance or the school's processes make it necessary data protection will form part of continuing professional development.

15. Monitoring Arrangements

This policy will be reviewed and updated when there are changes to GDPR and DPA 2108, guidance provided by case law or changes which will affect QfL's practice.

16. Links with Other Documents

This policy links with the following documents:

- QfL Homeworking Guidelines
- QfL Privacy Notice – Workforce
- QfL Privacy Notice – Pupils, Parents and Carers
- QfL Records Management, Retention and Disposal Policy

Tamzin Einon
Head of Operations

September 2019

Appendix A
Data Breach Procedure

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

1. On finding a breach or potential breach, the charity or data processor must immediately notify the designated employee (DE) for data protection and the Director of the charity.

2. The DE will undertake an initial investigate to determine whether a breach has occurred. He / She will consider whether personal data has been accidentally or unlawfully:

    - Altered
    - Destroyed
    - Lost
    - Published or made available to an inappropriate audience
    - Stolen
    - Made available to unauthorised people

3. The DE is to brief the CEO.

4. The DE will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary.

5. The DE, along with the Director, will decide if the breach must be reported to the ICO. This will be judged on a case-by-case basis. The DE is to take into consideration whether the breach is likely to negatively affect people's rights and freedoms, cause them any physical, material or non-material damage (e.g. emotional distress) through:

    - Damage to reputation
    - Discrimination
    - Financial loss
    - Identify theft or fraud
    - Loss of confidentiality
    - Loss of control over their data
    - Unauthorised reversal of pseudonymisation (for example, key-coding)
    - Any other significant economic or social disadvantage to the individual(s) concerned

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

6. The DE will document the decision (either way), in case it is challenged later by the ICO or an individual affected by the breach. Documented decisions are stored in a spreadsheet on QfL's computer network.

7. Where the ICO must be notified, the DE will complete the 'report a breach' page on the ICO's website within 72 hours. As required, the DE will set out:

    a) A description of the nature of the personal data breach including, where possible:

        - The categories and approximate number of individuals concerned
        - The categories and approximate number of personal data records concerned

    b) The name and contact details of the DE.

    c) A description of the likely consequences of the personal data breach.

d) A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned.

If all the above details are not yet known, the DE will report as much as he/she can within the 72 hours timeframe. The report will explain there is a delay, the reasons why, and when the DE expects to have further information. The DE will submit the remaining information as soon as possible.

8. The DE will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DE will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:

    a) The name and contact details of the DE
    b) A description of the likely consequences of the personal data breach
    c) A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned

9. The DE will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies.

10. The DE will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:

    a) Facts and cause
    b) Effects
    c) Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)
    d) Records of all breaches will be stored spreadsheet on QfL's computer network

11. The DE and Director will meet to review the breach and lessons learnt. This meeting will happen a soon as reasonably practicable.