1- Data Protection Policy - Quareia

Definitions

Last updated	24/05/2019

Organisation	means Quareia
GDPR	means the General Data Protection Regulation.
Responsible Person	means Quareia School Director.
Register of Systems	means a register of all systems or contexts in which personal data is processed by the organisation.

1. Data protection principles

The organisation is committed to processing data in accordance with its responsibilities under the GDPR. Article 5 of the GDPR requires that personal data shall be:

1. processed lawfully, fairly and in a transparent manner in relation to individuals;
2. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
3. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
4. accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
5. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and
6. processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures."

2. **Freedom of Information Request**

The Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004 SI No. 3244 (known as the Fees Regulations for brevity) section 9.

Under Fees Regulation 6(3) **Quareia reserves the right to charge a fee for information requests,** to cover the costs of:

• Reproducing any document containing the information, e.g. printing or photocopying;
• Postage and other forms of transmitting the information; and
• Complying with section 11 of FOIA where the applicant has expressed a preference for the means of communication and where this is reasonably practicable.

These costs are referred to as ‘communication costs’ or disbursements and are limited to expenses actually incurred.

2. General provisions

a- This policy applies to all personal data processed by the Organisation.
b- The Responsible Person shall take responsibility for the Organisation’s ongoing compliance with this policy.
c- This policy shall be reviewed at least annually.
d- The Organisation shall register with the Information Commissioner’s Office as an organisation that processes personal data.

3. Lawful, fair and transparent processing

a- Individuals have the right to access their personal data and any such requests made to the Organisation shall be dealt with in a timely manner.

4. Lawful purposes

a- All data processed by the Organisation must be done on one of the following lawful bases: consent, contract, legal obligation, vital interests, public task or legitimate interests (see ICO guidance for more information).
b- The Organisation shall note the appropriate lawful basis in the Register of Systems.
c- Where consent is relied upon as a lawful basis for processing data, evidence of opt-in consent shall be kept with the personal data.
d- Where communications are sent to individuals based on their consent, the option for the individual to revoke their consent should be clearly available and systems should be in place to ensure such revocation is reflected accurately in the Organisation’s systems.

5- Data minimisation

a. The Organisation shall ensure that personal data are adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

6- Right to erasure, to restrict processing, to rectification and to object

In certain circumstances data subjects have the right to have their data erased. This only applies:

- where the data is no longer required for the purpose for which it was originally collected, or
- where the data subject withdraws consent, or
- where the data is being processed unlawfully.

In some circumstances, data subjects may not wish to have their data erased but rather have any further processing restricted. If personal data is inaccurate, data subjects have the right to require Quareia to rectify inaccuracies. In some circumstances, if personal data are incomplete, the data subject can also require the controller to complete the data, or to record a supplementary statement.

Data subjects have the right to object to specific types of processing such as processing for direct marketing, research or statistical purposes. The data subject needs to demonstrate grounds for objecting to the processing relating to their particular situation except in the case of direct marketing where it is an absolute right.

7. Accuracy

a- The Organisation shall take reasonable steps to ensure personal data is accurate.
b- Where necessary for the lawful basis on which data is processed, steps shall be put in place to

ensure that personal data is kept up to date.

8. Archiving / removal

a- To ensure that personal data is kept for no longer than necessary, the Organisation shall put in place an archiving policy for each area in which personal data is processed and review this process annually.

b- The archiving policy shall consider what data should/must be retained, for how long, and why.

9. Security

1. The Organisation shall ensure that personal data is stored securely using modern software that is kept-up-to-date.
2. Access to personal data shall be limited to personnel who need access and appropriate security should be in place to avoid unauthorised sharing of information.
3. When personal data is deleted this should be done safely such that the data is irrecoverable.
4. Appropriate back-up and disaster recovery solutions shall be in place.

10. Breach

1- In the event of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data, the Organisation shall promptly assess the risk to people's rights and freedoms and if appropriate report this breach to the ICO.

END OF POLICY