Data Protection Policy

IQualify UK's Data Protection Policy is binding on all staff and students, and specifies the steps which iQualify UK is taking to conform to the requirements of the Data Protection Act (2018) and the General Data Protection Regulations.

Definitions

GDPR	Means the General Data Protection Regulation.
Responsible Person	Means the CEO.
Register of Systems	Means a register of all systems or contexts in which personal data is processed by iQualify UK.

1. Scope of the Policy

IQualify UK needs to collect certain types of personal information about the people with whom it deals, such as current, past and prospective students, employees, and those with whom it communicates. This information has to be collected for administrative purposes (such as staff recruitment and the administration of programmes of study), and to fulfil legal obligations to funding bodies and the government. The GDPR requires that this information should be processed fairly, stored safely and not disclosed to any other person unlawfully. IQualify UK is committed to protecting the rights and privacy of individuals in accordance with the requirements of the GDPR.

This document outlines iQualify UK's policies in relation to the GDPR.

IQualify UK's Data Protection Policy applies to all students and staff of iQualify UK. Any breach of the policy may result in iQualify UK, as the registered data controller, being liable in law for the consequences of the breach. Legal liability may also extend to the individual processing the data and his/her Head of Department or line manager under certain circumstances. In addition, breach of iQualify UK's Data Protection Policy by staff or students will be considered to be a disciplinary offence and will be dealt with according to iQualify UK's disciplinary procedures. Any member of staff or student who considers that the policy has not been followed with respect to personal data about themselves should raise the matter with their head of department.

This policy applies to all personal data for which iQualify UK is responsible, including electronic data and manual data which are covered by the GDPR. It applies regardless of where the data are held, and regardless of the ownership of the equipment used for processing, if the processing is performed for iQualify UK purposes. Outside agencies and individuals who work with iQualify UK, and who have access to personal information for which iQualify UK is responsible, will be expected to comply with this policy and with the GDPR.

2. Status of the Policy
This policy statement has been adopted by iQualify UK.

3. Data protection principles
IQualify UK is committed to processing data in accordance with its responsibilities under the GDPR. Article 5 of the GDPR requires that personal data shall be:

a. processed lawfully, fairly and in a transparent manner in relation to individuals;
b. 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;
c. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
d. 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;
e. 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
f. 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."

4. General provisions

a. This policy applies to all personal data processed by iQualify UK.
b. The Responsible Person shall take responsibility for iQualify UK's ongoing compliance with this policy.
c. This policy shall be reviewed at least annually.
d. iQualify UK is registered with the Information Commissioner's Office (ICO) as an organisation that processes personal data.

5. Lawful, fair and transparent processing

a. To ensure its processing of data is lawful, fair and transparent, iQualify UK shall maintain a Register of Systems.
b. The Register of Systems shall be reviewed at least annually.
c. Individuals have the right to access their personal data and any such requests made to iQualify UK shall be dealt with in a timely manner.

6. Lawful purposes

a. All data processed by iQualify UK must be done on one of the following lawful bases: consent, contract, legal obligation, vital interests, public task or legitimate interests.
b. iQualify UK 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 iQualify UK's systems.

7. Data minimisation

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

8. Accuracy

a. iQualify UK 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.

9. Archiving / removal

a. To ensure that personal data is kept for no longer than necessary, iQualify UK 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.

10. Security

a. iQualify UK shall ensure that personal data is stored securely using suitable software that is kept-up-to-date.
b. 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.
c. When personal data is deleted this should be done safely such that the data is irrecoverable.
d. Appropriate back-up and disaster recovery solutions shall be in place.

11. Breach

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, iQualify UK shall promptly assess the risk to people's rights and freedoms and if appropriate report this breach to the ICO.

12. Staff responsibilities

IQualify UK as a corporate body is a data controller under the GDPR. IQualify UK's Directors have oversight of planning and policy development matters in the area of information compliance, including data protection. The Principal deals with day to day data protection matters, such as subject access requests, and is a point of contact for issues relating to data protection.

When processing personal data, iQualify UK staff must ensure that they abide by the GDPR, this policy and any related policies. IQualify UK must only process personal data in accordance with its registration with the Information Commissioner. The registration defines the purposes for which IQualify UK processes personal data and related information, and is available on the Information Commissioner's website as part of the Register of Data Controllers.

In practice, most routine uses of personal data will be covered by iQualify UK's registration and will be legitimate from a data protection standpoint. However, this will not necessarily be the case where changes are introduced to the way in which data are processed - such as using the data for a purpose for which the data have not previously been used, or transferring the data to a new source.

Before such changes are introduced, staff should check to ensure that the proposed changes will be in accordance with iQualify UK's registration with the Information Commissioner, and will comply with the GDPR and this Policy. Staff who are uncertain as to whether their processing of data meets these requirements should refer any queries to their head of department or line manager in the first instance. Staff should also ensure that any personal information for which they are responsible is

accurate and up to date, including information which iQualify UK holds about themselves (e.g. their home address), and that data for which they are responsible is kept secure and are not disclosed to unauthorised parties.

Data should only be transferred internally within iQualify UK when there is a genuine business need to do so. Staff who receive transferred data are equally responsible for ensuring that the data are processed in accordance with this policy and iQualify UK's obligations under the GDPR. It is important that internally transferred data should continue to be used for purposes which are consistent with the purposes which applied when the data was gathered, to avoid violation of the GDPR. Particular care should be taken when disclosing personal data to parties outside iQualify UK.

Heads of Department and managers of administrative departments are responsible for ensuring that the processing of personal data in their department conforms to the requirements of the GDPR and this policy. In particular, they should ensure that new and existing staff who are likely to process personal data are aware of their responsibilities under the Act. This includes drawing the attention of staff to the requirements of this policy, and ensuring that staff who have responsibility for handling personal data are provided with adequate training.

Managers must also see that correct information and records management procedures are followed in their departments. This includes establishing retention periods to ensure that personal data are not kept for longer than is required.

Staff should also note that iQualify UK is not responsible for any processing of personal data by them which is not related to their employment with iQualify UK, even if the processing is carried out using iQualify UK's equipment and facilities. Staff are personally responsible for complying with the GDPR in regard to data for which they are the data controller.

13. Gathering data

Any gathering of personal data by members of iQualify UK must be accordance with iQualify UK's registration with the Information Commissioner. Staff should check the Register of Data Controllers on the Commissioner's website (or check with a Director) before introducing any new form of data gathering or making changes to existing methods of data gathering. If it appears that the collection of the data would not be covered by iQualify UK's existing registration, the Director must be informed before the changes are implemented, so that iQualify UK's register entry can be updated.

To meet these requirements, paper and electronic forms (including web based forms) created by iQualify UK which gather personal data should always include a fair processing notice.

Information about visitors to a website gathered through cookies, web bugs and other devices will become personal data if the data is linked to personal details of the user, such as name and address details submitted through an online form. IQualify UK websites which use cookies, web bugs and other tracking devices in this way should include a privacy statement explaining:

- Which data will be collected in this way
- Which parts of iQualify UK will use the data
- How the data will be used
- How long the data will be kept
- How users can disable cookies, web bugs and other devices if they wish to do so
- For further information on cookies and web bugs, see the iQualify UK website's Privacy Policy

14. Disclosure of data
Staff must take particular care when disclosing personal data to third parties, to ensure that there is no breach of the GDPR or the law of confidence.

Disclosure may be unlawful even if the third party is a family member of the data subject, or a local authority, government department or the police. A key point to consider is whether the disclosure is relevant to and necessary for the conduct of iQualify UK's business. For example, it would generally be appropriate to disclose a staff member's work contact details in response to an enquiry relating to a function for which they are responsible, but it would not be reasonable or appropriate to disclose a staff member's personal address or bank account details.

Staff should always exercise caution when dealing with requests from third parties for the disclosure of personal data. Disclosure requests should normally be required to be in writing, and should be responded to in writing. Where reasonable, the party making the request should be required to provide a statement explaining the purpose for which the data is requested, the length of time for which the data will be held, and an undertaking that the data will be held and processed according to the GDPR.

Where the request relates to the prevention/detection of crime, the apprehension/prosecution of offenders, assessment/collection of any tax or duty, or the discharge of regulatory functions, appropriate paperwork should be produced by the enquirer to support their request (e.g. official documentation stating that the information is required in support of an ongoing investigation).

Personal data should only be disclosed over the telephone in emergencies, where the health or welfare of the data subject would be at stake. If data have to be disclosed by telephone, it is good practice to ask the enquirer for their number and to call them back.

Particular care should be taken when dealing with requests from embassies and high commissions, as data subjects may choose to have little or no contact with representatives of their home states. Similarly, iQualify UK students may have reasons for not wanting contact with parents, other relatives or friends. Requests from relatives, friends etc. for the contact details of students should therefore be treated with caution. It is good practice to offer to pass on any message without providing contact details or confirming or denying that the person is an iQualify UK student.

An image of an identifiable individual is personal data about them. In some situations, publication of an image without the individual's permission with infringe their right to privacy and the GDPR.

Individuals have the right to access their personal data:

- This is commonly referred to as subject access.
- Individuals can make a subject access request verbally or in writing.
- A request must be responded to within one month.
- There is no fee charged to deal with a request.

15. Security of data
The GDPR requires that precautions should be taken against the physical loss or damage of personal data, and that access to and disclosure of personal data should be restricted. IQualify UK staff who are responsible for processing personal data must ensure that personal data are kept securely, and that personal information is not disclosed orally or in writing, by accident or otherwise, to unauthorised third parties.

Information security is a large area, so the following recommendations are meant as general guidance only. They apply equally to data processed off-site (e.g. by staff at home, on a phone or on laptops), as to data processed on iQualify UK's premises. In fact, off-site processing presents a potentially greater risk of accidental loss, theft or damage to data.

Manual data

- When not in use, files containing personal data should be kept in locked stores or cabinets to which only authorised staff have access.
- Procedures for booking files in and out of storage should be developed, so that file movements can be tracked.
- Files should be put away in secure storage at the end of the working day, and should not be left on desks overnight.

Electronic data

Care must be taken to ensure that PCs and terminals on which personal data are processed are not visible to unauthorised persons, especially in public places. Screens on which personal data are displayed should not be left unattended. Particular care must be taken when transmitting personal data. Appropriate security precautions, such as the use of encryption and digital signatures, should be taken when sending personal data by email. Transmission of personal data by fax should generally be avoided.

IQualify UK students using iQualify UK's Teaching Zone must conform to iQualify UK's Data Protection Policy

16. References and recruitment

Confidential references for educational or employment purposes will involve the disclosure of personal information, often of a private nature. Requests for references which are received from reputable organisations and which request that the reference is returned to a recognised address can generally be taken at face value, where it is known that the individual who is the subject of the request has cited an iQualify UK employee as a referee. However, if there is any doubt as to the validity of a reference request, staff should always check with the individual concerned to determine that they are willing for information about them to be released.