iQuda data protection policy

Context and overview

Introduction

iQuda needs to gather and use certain information about individuals. These individuals can include customers, suppliers, business contacts, employees and other people the organisation has a relationship with or may need to contact.

This policy describes how this personal data must be collected, handled and stored to meet the company's data protection standards — and to comply with the law.

Why this policy exists

This data protection policy ensures that iQuda:

- Complies with data protection law and follow good practice
- Protects the rights of staff, customers and partners
- Is open about how it stores and processes individuals' data
- Protects itself from the risks of a data breach

Data protection law

The General Data Protection Regulations 2016 describes how all organisations must collect, handle and store personal information.

These rules apply regardless of whether data is stored electronically, on paper or on other materials.

To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully.

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."

People, risks and responsibilities

Policy scope

This policy applies to:

- The head office of iQuda
- All current or future branches of iQuda
- All staff and volunteers of iQuda
- All contractors, suppliers and other people working on behalf of iQuda

It applies to all data that the company holds relating to identifiable individuals, even if that information technically falls outside of the General Data Protection Regulations 2016. This can include:

- Names of individuals
- Postal addresses
- Email addresses
- Telephone numbers
- ...and also any other information relating to individuals

Data protection risks

This policy helps to protect iQuda from some very real data security risks, including:

- **Breaches of confidentiality.** For instance, information being given out inappropriately.

- **Failing to offer choice.** For instance, all individuals should be free to choose how the company uses data relating to them.

- **Reputational damage.** For instance, the company could suffer if hackers successfully gained access to sensitive data.

Responsibilities

Everyone who works for or with iQuda has a responsibility for ensuring data is collected, stored and handled appropriately.

Each team that handles personal data must ensure that it is handled and processed in line with this policy and data protection principles.

However, these people have key areas of responsibility:

- The **board of directors** is ultimately responsible for ensuring that iQuda meets its legal obligations.

- The **Data Protection Officer, Garth Macintosh**, is responsible for:

    - Keeping the board updated about data protection responsibilities, risks and issues.

    - Reviewing all data protection procedures and related policies, in line with an agreed schedule.

    - Arranging data protection training and advice for the people covered by this policy.

    - Handling data protection questions from staff and anyone else covered by this policy.

    - Dealing with requests from individuals to see the data iQuda holds about them (also called 'subject access requests').

    - Checking and approving any contracts or agreements with third parties that may handle the company's sensitive data.

    - Approving any data protection statements attached to communications such as emails and letters.

    - Addressing any data protection queries from journalists or media outlets like newspapers.

    - Where necessary, working with other staff to ensure marketing initiatives abide by data protection principles.

- The **Technical Director, James Watson**, is responsible for:

    - Ensuring all systems, services and equipment used for storing data meet acceptable security standards.

- Performing regular checks and scans to ensure security hardware and software is functioning properly.

- Evaluating any third-party services the company is considering using to store or process data. For instance, cloud computing services.

General staff guidelines

- The only people able to access data covered by this policy should be those who **need it for their work.**

- Data **should not be shared informally**. When access to confidential information is required, employees can request it from their line managers.

- iQuda **will provide training** to all employees to help them understand their responsibilities when handling data.

- Employees should keep all data secure, by taking sensible precautions and following the guidelines below.

- In particular, **strong passwords must be used** and they should never be shared.

- Personal data **should not be disclosed** to unauthorised people, either within the company or externally.

- Data should be **regularly reviewed and updated** if it is found to be out of date. If no longer required, it should be deleted and disposed of.

- Employees **should request help** from their line manager or the data protection officer if they are unsure about any aspect of data protection.

Data storage

These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to the IT manager or data controller.

When data is **stored on paper**, it should be kept in a secure place where unauthorised people cannot see it.

These guidelines also apply to data that is usually stored electronically but has been printed out for some reason:

- When not required, the paper or files should be kept **in a locked drawer or filing cabinet.**

- Employees should make sure paper and printouts are **not left where unauthorised people could see them**, like on a printer.

- **Data printouts should be shredded** and disposed of securely when no longer required.

When data is **stored electronically**, it must be done so on "iQuda" supplied "Encrypted" device only.

- Data should be **protected by strong passwords** that are changed regularly and never shared between employees.
- If data is **stored on removable media** (like a CD or DVD), these should be kept locked away securely when not being used.
- Data should only be stored on **designated drives and servers** and should only be uploaded to **approved cloud computing services**.
- Servers containing personal data should be **sited in a secure location**, away from general office space.
- Data should be **backed up frequently**. Those backups should be tested regularly, in line with the company's standard backup procedures.
- All servers and computers containing data should be protected by **approved security software and a firewall.**

Data use

Personal data is of no value to iQuda unless the business can make use of it. However, it is when personal data is accessed and used that it can be at the greatest risk of loss, corruption or theft:

- When working with personal data, employees should ensure **the screens of their computers are always locked** when left unattended.
- Personal data **should not be shared informally**. In particular, it should never be sent by email, as this form of communication is not secure.
- Data must be **encrypted before being transferred electronically**. The IT manager can explain how to send data to authorised external contacts.
- Personal data should **never be transferred outside of the European Economic Area**.
- Employees **should not save copies of personal data to their own computers**. Always access and update the central copy of any data.

Data accuracy

The law requires iQuda to take reasonable steps to ensure data is kept accurate and up to date.

The more important it is that the personal data is accurate, the greater the effort iQuda should put into ensuring its accuracy.

It is the responsibility of all employees who work with data to take reasonable steps to ensure it is kept as accurate and up to date where ever possible.

- Data will be held in **as few places as necessary**. Staff should not create any unnecessary additional data sets.

- Staff should **take every opportunity to ensure data is updated**. For instance, by confirming a customer's details when they call.

- iQuda will make it **easy for data subjects to update the information** iQuda holds about them. For instance, via the company website.

- Data should be **updated as inaccuracies are discovered**. For instance, if a customer can no longer be reached on their stored telephone number, it should be removed from the database.

- It is the marketing manager's responsibility to ensure **marketing databases are checked against industry suppression** files every six months.

Subject access requests

Individuals are legally entitled to ask iQuda to confirm whether the company is processing data about them, and to request a copy of the data. This will be provided in a commonly used format such as a PDF, Word, or Excel document.
iQuda may charge a reasonable fee to cover the administrative costs to provide an individual with their data, if their request is manifestly unfounded or excessive. In this circumstance, iQuda will not release their data until the fee is paid. iQuda will comply with all Subject Access Requests within 30 days of receipt.
Subject access requests should be submitted by email or by post to "The Data Protection Officer", and sent to the postal address or email address listed below:
Post

Data Protection Officer
iQuda
Unit 3 Heron Business Park
Eastman Way
Hemel Hempstead
Hertfordshire
HP2 7FW

Email

info@iquda.co.uk

Disclosing data for other reasons

In certain circumstances, the General Data Protection Regulations allow personal data to be disclosed to law enforcement agencies without the consent of the data subject.

Under these circumstances, iQuda will disclose requested data. However, the data controller will ensure the request is legitimate, seeking assistance from the board and from the company's legal advisers where necessary.

Providing information

iQuda aims to ensure that individuals are aware that their data is being processed, and that they understand:

- How the data is being used
- How to exercise their rights

To these ends, the company has a privacy statement, setting out how data relating to individuals is used by the company.

This privacy policy is available on the company website in the following location: https://www.iquda.co.uk/privacy-cookie-policy/

Practical Guidelines

Do:	Don't
• Seek advice from your line manager or an iQuda director if you are unclear about any aspect of information security.	• Disclose your password to anyone or ever share passwords.
• Report any loss or suspected loss of data to your line manager or an iQuda Director.	• Use a personal email account for conducting iQuda business.
• Change your password if you have any suspicion that it may have been compromised.	• Use an iQuda email account for conducting personal business or use iQuda email distribution lists for personal emails.
• If you use iQuda supplied portable media to store or process data pertaining to iQuda or its clients, destroy the data securely when you have finished using it. At end of life all electronic files must be multi pass patterns wiped to HMG S5 onsite prior to disposal and degaussed or physically destroyed.	• Make copies of restricted iQuda information without permission.
• Mobile devices are encrypted to at least	• Provide access to iQuda information or systems to those who are not entitled to

Do:	Don't
AES25.	access.
• Password protect your personally owned devices.	• Undermine or seek to undermine the security of computer systems, for example, by installing unauthorized software..
• Keep all of the software on your personally owned devices up to date and install anti-virus protection.	• Leave your computers unlocked when left unattended.
• Comply with the law and iQuda policies.	• Leave hard copies of confidential information unattended or unsecured.
• Be mindful of the risks of using open (unsecured) Wi-Fi hotspots or computers in internet cafes, public libraries etc.	• Assume that Information Security is someone else's responsibility. **It is the responsibility of all iQuda staff.**
• All data including backups are encrypted to at least AES256.	• Access websites known to be infected with viruses or suspicious materials. • Access websites that are unacceptable at work (e.g. containing pornographic, explicit or illegal content).
• Report any suspicious occurrences, such as the appearance of viruses, Ransomware, Trojans or other malicious computer threats.	• Fail to report suspicious occurrences, even if you aren't sure of their severity.