iQuda information classification & handling policy

Purpose

This iQuda policy provides a framework for ensuring that information; regardless of its form, is valued, classified and handled appropriately, in line with the requirements of the Data Protection Act (2018) and the General Data Protection Regulations (2016). This policy applies to all data held by iQuda. The policy will determine how data should be classified and handled, that information assets are appropriately and adequately protected.

Scope

This policy applies to all data and information held by iQuda, regardless of its form or source. This includes paper, electronic, verbal and multi-media information assets. Example information assets include, but are not limited to; documents, voice recordings, videos, spreadsheets, files, printed documents, data backups and all future data formats. The policy applies to data owned by iQuda, or its staff, or its clients.

This policy applies to all employees, work experience placements, data processes, associates and all other third parties working at or in partnership with iQuda. Each individual is personally responsible for ensuring that they correctly classify and handle information. The iQuda management team are responsible for ensuring that this policy is brought to the attention of these third parties.

Underlying Principles

- This policy forms part of the other policies enforced at iQuda.
- Information assets are valuable to iQuda's staff, clients, other stakeholders and to iQuda as a whole. It is therefore important that these assets are suitably protection.
- Information assets could cause damage to iQuda if classified or handled incorrectly.
- It is essential for iQuda to apply with its legal obligations, including but not limited to: The Data Protection Act 2018 and the General Data Protection Regulations 2016.
- Information assets should only be accessed by legitimate parties and for legitimate reasons. On the reverse, access should be prevented for illegitimate parties.
- Care should be taken by all parties employed by or working at or on behalf of iQuda.
- Devices containing information and data must be wiped to at least HMG S5 standards after use. Retired computers/devices are overwritten with 7 passes before being physically destroyed. At end of life all electronic files must be multi pass patterns wiped to HMG S5 on site prior to disposal and degaussed or physically destroyed.

Categories

Data is classified according to the level sensitivity it holds and the impact that it's unauthorized disclosure, alteration, loss or destruction will have on iQuda and iQuda's stakeholders. Data is classified in this way to ensure that those individuals who have a legitimate reason to access an information asset can do so, whilst ensuring that the information asset is protected from individuals or organizations who do not have a legitimate reason to access the data.

All information assets held or used by iQuda can be categorized into one of the following four categories:

- Public
- Internal
- Confidential
- Sensitive Confidential

Please see the Data Classification Table on the next page.

	Public	Internal	Confidential	Sensitive Confidential
Description	Can be viewed by anyone without causing damage.	Can be viewed by anyone working at iQuda, but normally would be unavailable to those outside of iQuda.	Accessible only be approved individuals on a need to know basis (where knowledge is pertinent for business purposes).	Accessible only to upper management, business owners and staff who are currently performing supervised work on their behalf. This information could be damaging to iQuda, it's staff, clients or other stakeholders if inappropriately distributed or used.
Level of Risk	None.	Low.	Medium.	High.
Controls	None. Info widely available.	For internal use only, should not be distributed outside of iQuda without prior management consent.	Access restricted to a small number of individuals who need the information in order to complete their work.	Dissemination restricted to authorized individuals only.
Storage & Security	Can be stored on any device (in accordance with other iQuda policy). No restrictions on printing, copying or distributing, subject to copyright or other applicable laws.	Should be stored on iQuda's intranet or on iQuda approved and encrypted devices, including PCs, laptop or external data storage devices. Paper copies should not be left lying around unattended.	Information should be sorted on password restricted shared folders on the iQuda network, or in password restricted sections of the intranet, or on encrypted devices, signed for and authorized by iQuda management. Paper copies should not be left unattended.	Information should be stored on password restricted shared folders on the iQuda network, or in password restricted sections of the intranet, or on encrypted devices owned or managed by the managing director or business owners. Paper copies should be limited and locked away when not in use.
Transmission	No restriction (in accordance with other iQuda policy).	Send via internal email only unless otherwise approved by Senior Management.	Transmission through secured shared locations. Can be transmitted by email between authorized individuals only. All relevant recipients should be CCd.	Should only be transmitted electronically in an acceptably encrypted format*. Hard copies of documents should be hand delivered internally. External postage should be signed for.
Disposal	No restrictions.	Paper copies should be shredded securely. Electronic copies should be deleted and double-checked.	Paper copies should be shredded securely. Ensure that electronic copies are deleted and devices wiped clean.	Paper copies should be shredded securely. Ensure that electronic copies are deleted and devices reformatted.
Examples of Data (including but not limited to)	Any information on the iQuda website. Information contained within publicly available publications (e.g. company publications or sales brochures). Press releases	Internal correspondences Internal procedures or policies containing specific information that would not normally be made available publically for example business plans & disaster recovery documentation	Documents containing sensitive personal or company data Management Data Sensitive, restricted Financial Data. Proposed company changes.	Confidential records Information pertaining to lawsuits or legal issues HR Data Disciplinary proceedings Passwords Security information

	Company policies containing general information that could not cause damage if disclosed. Example policies include our password policy, our information classification & handling policy & other policies which contain general information about company approaches.	Any document containing specific information about the company network, company departments or other information that could be beneficial to our competitors. Uncompleted work forms such as leave forms. Non-sensitive company announcements.		Safe Key Code

Responsibilities

All data or information should have an owner i.e. an author or the service line manager. This is to ensure that responsibility can be attributed and managed by a single person or a limited number of people.

We recognise that it is not feasible to classify every piece of information within iQuda. However it is vital that all employees are aware of the classification system. This ensures that due diligence can be maintained through the organization. It will likely be obvious which type of information should be treated confidentially, but for the avoidance of doubt please speak to the Information Governor, Anthony Jones. When there is doubt, it is expected that information is treated as “sensitive confidential” in the first instance.

All staff working at iQuda have a responsibility for ensuring that information and classified and handled appropriately.

Garth Macintosh the Data Protection Officer is responsible for labelling information is accordance with the Data Classification Table.

All staff who are involved in the creation, editing or reissue of company documents must ensure that they label and handle documents or data correctly.

Relevant Policies

This Information Classification and Handling Policy must be used in combination with all other policies enforced at iQuda. No other policy can be unconsidered when classifying or handling information at iQuda.

Formal Document Labelling and Storage

All formal documentation used at iQuda, must be labeled correctly. This helps to ensure that documents can be tracked, issued and reviewed in the correct manner. Document classification also ensures that the correct version of each document is always in use, and that older versions can be removed from circulation when they are no longer relevant. The majority of these formal documents are:

- Policies
- Forms e.g. Leave request, Change requests, Change Reviews, Training

- Employment Forms e.g. Health and Safety, Interview Forms, Candidate Assessment Forms etc.
- Process documents

All formal documents should include a header or footer which contains the following information:

- Data classification label e.g. Public, Internal, Confidential or Sensitive Confidential.
- Date of creation
- Date of version
- Date of next review
- Name of person(s) who created the document
- Name of person who approved the document
- Version number
- Document name

All formal documents are stored on SharePoint.
All staff can access relevant forms and policies on SharePoint.
Certain forms and formal documents are for management use only. These can be found on SharePoint.