Title	**Data Privacy & Protection Policy**
Owner	**Services Committee Chair/Director**
Version Number	Version 2.0
Primary Audience	The Primary Audience of this policy is those responsible for Data Management (i.e. The PR & Fundraising Coordinator; Volunteer coordinator, Finance Administrator; and, the General Management Team within QCCC. All colleagues within QCCC also need to be familiar with this Policy and its supporting documentation and processes.

Introduction and Objectives

QCCC has a moral, legal and regulatory responsibility to protect the privacy of individuals who provide us with personal information.

This policy: -

a) highlights the framework within which QCCC will meet regulatory requirements in accordance with:
   - The Data Protection Act 1998;
   - The Data Protection Act 2018; and,
   - The EU General Data Protection Regulation (GDPR) (2018).

b) explains clearly the responsibilities of:
   - those directly involved in or accountable for Data within QCCC;
   - all colleagues and volunteers; and,
   - our suppliers and service providers

c) provides clear direction and requirements to ensure a consistent and effective approach to QCCC's data management.

Scope

The requirements of the policy apply to all colleagues and volunteers within QCCC and to all aspects of QCCC's operational services including Governance and Board Committee activities. They also apply to any outsourced service providers or suppliers with whom QCCC may be contractually or legally obliged to share Personal data.

Out of Scope

QCCC operates in North West Edinburgh within the United Kingdom and will not transfer any data to other jurisdictions outwith the UK.

The Freedom of Information Act 2000 (FOI) created a new category of data which extended the definition of "data" in the Data Protection Act to include any information held by a public authority which would not otherwise be caught by the definition.

Risk Appetite Alignment

QCCC is committed to an environment & culture which protects the rights and privacy of all individuals connected to QCCC. QCCC is keen to ensure effective application of data management maintaining efficient business operations while protecting our clients, and has minimal appetite for any adverse operational impacts as a result of lack of access to data caused by system downtime/failure.

QCCC's has zero appetite for data privacy events resulting from failure to:

- protect the confidentiality, integrity and availability of personal information;
- comply with individual's rights under data privacy law; and,
- stop inappropriate use of its information systems and the personal information held on these systems.

There is no appetite to deviate from this policy. Any breach of The Data Protection Acts or QCCC's Data Protection Policy could result in disciplinary procedures. Serious cases may also constitute a criminal offence.

Requirements

Data may be held by QCCC for the following purposes:

- Staff Administration.
- Day Care Administration
- Volunteer Administration
- Fundraising
- Accounts and Recording/Financial
- Advertising, Marketing and Public Relations, including Social Media
- Research

Personal Data and Sensitive Personal Data

To provide our services QCCC must gather and store Personal Data including some Sensitive Personal Data. This is in order to provide a more holistic service to our service users and to develop the service user's personal plan.

QCCC will maintain:

- a Data recovery plan
- a data map,
- a Subject Access Request procedure
- an information Asset & Records Retention Schedule
- a breach register,
- a published Privacy Notice;
- ICO registration
- an IT Server recovery and restore contract
- a Computer Backup Procedure

Requirements continued

All Personal Data – will be maintained in accordance with the GDPR, Privacy and Data Protection Act(s) Principles detailed in the Appendix to this Policy, and covering: -

- Lawful, Fair and Transparent
- Purpose, Adequacy, Limitation and Minimisation
- Accuracy
- Retention, Storage and Transmission
- Security, Integrity and confidentiality
- Accountability
- Data Standards and Training

Fair & Lawfully Processing –

- The QCCC logo will feature on all correspondence,
- Contract documentation will state our intentions on processing the data and state if, and to whom, we intend to share the personal data with.
- Where possible we will also provide an indication of the duration the data will be kept

Processing for Limited Purpose –

- QCCC will not use data for purposes other than those agreed by individuals involved. If data held by us is requested by external organisations (for any reason) this will only be passed upon written permission from the individuals involved. However, on occasion we may share information, without receiving prior consent, with Health/Social care and/or the Police if we feel an individual is 'at risk' of harm or abuse or where QCCC has a legal obligation to do so.

Adequate, Relevant and Not Excessive –

- Information will be held in accordance with the retention periods set out in the QCCC Information Asset Register.
- QCCC will monitor the data held for our purposes, ensuring we hold neither too much nor too little data in respect of the individuals about whom the data is held. If data given or obtained is excessive for such purpose, this will be immediately deleted or destroyed.

Accurate and Up-to-Date

- All amendments to individual information will be made immediately and data no longer required will be deleted or destroyed.
- It is the responsibility of both individuals and QCCC to ensure all data held by us is accurate and up-to-date. Completion of the appropriate form (provided by us) will be taken as an indication that the data contained is accurate.
- QCCC will update and provide our service users with a copy of their personal plan at least twice in any 12-month period

Requirements continued

Data will be processed in accordance with the individual's rights - All individuals that Queensferry Care holds data on have the right to:

- To submit a Subject Access Request regarding information held about them by QCCC;
- Prevent the processing of their data for the purpose of direct marketing;
- Be compensated if they can show that they have been caused damage by any contravention of the Act;
- Request the removal/correction of any inaccurate data about them.

Security of Information

- Appropriate technical and organisational measures will be taken against the unauthorised or unlawful processing of personal data and against accidental loss or destruction of data. These include;
    1. All information databases are password protected allowing only authorised personnel access
    2. All personal and financial data is stored securely allowing only authorised personnel access
- To mitigate the risks associated with paper processing QCCC will encourage: Paperless Working; Electronic Filing; Clean Desk Policy; Post not used for Personal Data; and, Faxing not used for Personal Data,
- If personal data is lost or compromised in any way staff/volunteers must report this to a Manager immediately.

Operational Resiliency - IT server backup copies will be taken regularly and must be held externally to QCCC's building(s).

Staff and Volunteer Training

As part of Staff & Volunteer inductions all individuals must receive training on the safe storage and handling of information. There is a dedicated section explaining data protection in the Staff/Volunteer and Member Handbook and all individuals are required to review, sign and return a form acknowledging the Handbook as part of their contract of employment. Mandatory training on 'Data Protection' for all individuals must be included in the QCCC training calendar.

Financial Data

Financial data is to be stored on a password protected computer in an encrypted file, or in a locked safe. QCCC employs an external supplier in the provision of Pay Roll & Pensions and therefore has to share financial data with third party organisations. In line with HMRC guidelines all financial data is retained for 7+ years. Bank details acquired for PAYE or standing order purposes are immediately passed to our financial provider. QCCC will not retain any personal bank details.

Privacy Impact Assessments

We ensure that any new system of procedure that contains Personal Data is stress tested to ensure it will be compliant with all of the above.

Responsibilities	
Services Committee Chair / Director	To review and revise the policy as and when necessary and to approve the Policy To ensure that risk-based monitoring plans are in place to verify the effective implementation of QCCC's Data Privacy Policy and Procedures To ensure that data privacy requirements are included at the start of any change management projects or any new use of personal information
Data Controllers	The Board of Directors of Queensferry Care have appointed the Management team as Data Controllers.
General Managers	As **Data Controllers** to "*determines the purposes for which and the manner in which any personal data are, or are to be, processed.*" To maintain and refresh the policy and ensure it reflects any changes in regulation To ensure arrangements are in place to maintain data and supporting documentation including: - • completion of Privacy Risk Impact assessments • an audit trail of data privacy notices used. • a breach register • an information Asset & Records Retention Schedule • a data map To implement risk-based monitoring plans and conduct annually, as a minimum, a desktop walkthrough test of data processes, reporting any issues identified to the Services Committee.
General Managers, Service Leads **and all colleagues** involved in provision of services to Clients, Fundraising or Marketing	**Data Privacy Management Requirements: -** **1. Fair & Lawful processing** 1.1. Only collect personal information where there is a valid business reason for doing so, and where necessary, obtain the individual's consent 1.2. Through a compliant data privacy notice, inform an individual about how their personal information will be used. 1.3. Do not use personal information contrary to its original purpose or otherwise outside the individual's expectations 1.4. Ensure that any information shared is in line with the data privacy notice provided to the individuals.

Responsibilities continued

General Managers, Service Leads and all colleagues involved in provision of services to Clients, Fundraising or Marketing	**2. Data Quality** 2.1. Ensure personal information held is accurate and up to date 2.2. Delete or destroy personal information in line with the Records Management Policy requirements 2.3. Ensure that adequate, relevant but not excessive information is collected to fulfil business objectives. **3. Respecting Individuals' Rights** 3.1. Ensure individuals' rights under privacy laws are respected and acted upon within statutory timescales These are: 3.1.1. Managing individuals' requests to access their personal information (e.g. Data Subject Access Request or DSAR, including providing the information the individual is entitled to. 3.1.2. Manage marketing preferences across all communication channels. 3.1.3. Respond to requests to amend personal information **4. Security & Personal Information** 4.1. Personal information must be protected against accidental or deliberate misuse, damage or destruction. 4.2. Ensure that disclosures of personal information are undertaken in compliance with the law, including maintenance of records to identify disclosure of personal information to third parties such as government bodies, health service agencies, police etc. with a clear explanation as to why the disclosure was valid. 4.3. Ensure that colleagues only access personal information where there is a valid business or legal/regulatory need to do so. 4.4. If personal information is lost or compromised in any way Staff/Volunteers must report this to a Manager immediately.

Key Controls & Indicators

Key Control(s)	Key Indicator(s)	Monitoring Frequency
Electronic devices where Personal Data is stored are encrypted and/or password protected.	All information databases are password protected allowing only authorised personnel access All personal and financial data is stored securely allowing only authorised personnel access	General Managers - Quarterly

Key Controls & Indicators continued		
Key Control(s)	**Key Indicator(s)**	**Monitoring Frequency**
Business Continuity & Disaster Recovery Plan in place	Reviewed within last 12 months	Report to Finance Committee July 2020 and annually thereafter
IT Weekly Backups completed	Managers/Administrators to confirm in Finance Committee reporting	Quarterly Reporting to Finance Committee
7 x 24 – Offsite IT recovery contract in place	Maintenance contract in place	IT issues monitored and reported to Finance Committee (quarterly) and Board (monthly)
Day Care Members sign a form to say that data protection and information sharing has been explained and is understood.	Managerial Checks as part of Induction checklist sign-off and Personal Plan reviews.	As and when new members join and half yearly personal plan reviews.

Supporting Materials and related policies

- IT Infrastructure and Disaster Recovery Plan plus Computer Backup Procedure
- Subject Access Rights Procedure
- Information Asset & Records Retention Register
- Data map (relating to article 30 of GDPR)
- Data Breech Procedure and Register
- Data Privacy Notice

Contact Points for Queries or Guidance:
Gillian Smith/Liz Mcintosh, General Managers

Version Control/History

Version No.	Author	Approval Date	Effective Date	Status/Comments
1.3	Andrew Burton		Sept 2017	Previous Policy Version
2.0	Iain Macdonald	1st Feb 2020	Immediate	Overarching policy created and enhanced based on review and consolidation of various principles and existing documentation.