GDPR01 - Overarching GDPR Policy and Procedure

Category: GDPR **Sub-category:** Policies

Policy Review Sheet

Review Date: 18/01/18 **Policy Last Amended:** 18/01/18

Next planned review in 12 months, or sooner as required.

Note: The full policy change history is available in your online management system.

Business Impact:	Low	Medium	High	Critical
			X	
These changes require action as soon as possible. Changes include fixed implementation dates which are detailed within the policy.				

Reason for this review:	New Policy
Were changes made?	Yes
Summary:	A detailed introduction to GDPR, setting out the documents that will be produced. The policy includes a journey map with the issues that should be considered and steps to take to achieve GDPR compliance. It refers at a high level to all the elements of GDPR that will be covered in each of the policies and procedures and guidance, as well as an explanation of the governance/enforcement of GDPR.
Relevant Legislation:	• The Data Protection Act 2018 • The General Data Protection Regulation 2016 (EU) 2016/679
Underpinning Knowledge - What have we used to ensure that the policy is current:	• Information Commissioner's Office, (2018), *Guide to the General Data Protection Regulation (GDPR)* [Online] Available from: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/ [Accessed: 16/01/2018] • Information Commissioner's Office, (2017), *Preparing for the General Data Protection Regulation (GDPR) - 12 steps to take now*. [Online] Available from: https://ico.org.uk/media/1624219/preparing-for-the-gdpr-12-steps.pdf [Accessed: 16/01/2018] • Information Commissioner's Office, (2018), *Health*. [Online] Available from: https://ico.org.uk/for-organisations/health/ [Accessed: 16/01/2018]
Suggested action:	• Encourage sharing the policy through the use of the QCS App • Establish process to confirm the understanding of relevant staff • Establish training sessions for staff • Arrange specific meetings to discuss the policy changes and implications • Ensure that the policy is on the agenda for all team meetings and staff handovers • Widely distribute the 'Key Facts' of the policy • Share content of the policy with all staff

GDPR01 - Overarching GDPR Policy and Procedure

This page is deliberately left blank

GDPR01 - Overarching GDPR Policy and Procedure

1. Purpose

1.1 The purpose of this policy is to ensure that QCS Client Ltd understands the key principles of the General Data Protection Regulation (GDPR).

1.2 This policy sets out the steps that need to be taken by QCS Client Ltd to ensure that QCS Client Ltd handles, uses and **processes personal data** in a way that meets the requirements of GDPR. It should be read alongside the suite of QCS Client Ltd GDPR policies, procedures and guidance.

1.3 This policy applies to all staff at QCS Client Ltd who process personal data about other staff, Service Users and any other living individuals as part of their role.

1.4 To support QCS Client Ltd in meeting the following Key Lines of Enquiry:

Key Question	Key Line of Enquiry (KLOE)
WELL-LED	HW1: Is there the leadership capacity and capability to deliver high-quality, sustainable care?
WELL-LED	HW4: Are there clear responsibilities, roles and systems of accountability to support good governance and management?
WELL-LED	W2: Does the governance framework ensure that responsibilities are clear and that quality performance, risks and regulatory requirements are understood and managed?
WELL-LED	W3: How are the people who use the service, the public and staff engaged and involved?

1.5 To meet the legal requirements of the regulated activities that QCS Client Ltd is registered to provide:

- The Data Protection Act 2018
- The General Data Protection Regulation 2016 (EU) 2016/679

2. Scope

2.1 The following roles may be affected by this policy:

- All staff

2.2 The following people may be affected by this policy:

- Service Users

2.3 The following stakeholders may be affected by this policy:

- Commissioners

GDPR01 - Overarching GDPR Policy and Procedure

3. Objectives

3.1 The objective of this policy is to ensure staff have a working knowledge into the principles and requirements of GDPR.

3.2 Alongside the suite of policies, procedures and guidance available QCS Client Ltd can demonstrate that appropriate steps are taken to ensure QCS Client Ltd complies with GDPR when handling and using personal data provided by both staff and Service Users.

3.3 This policy will assist with defining accountability and establishing ways of working in terms of the use, storage, retention and security of personal data.

3.4 This policy will assist with understanding the obligations of QCS Client Ltd in respect of the rights of the staff and Service Users who have provided personal data and the steps QCS Client Ltd should take if it breaches GDPR.

GDPR01 - Overarching GDPR Policy and Procedure

4. Policy

4.1 GDPR Background

GDPR came into force on the 25 May 2018 and replaced the Data Protection Act 1998. Regardless of the impact of Brexit, GDPR will remain. GDPR provides greater protection to individuals and places greater obligations on organisations, but can be dealt with in bite-size chunks to ensure that any impact on the provision of care and services is minimised.

4.2 All staff need to ensure the ways in which they handle personal data meet the requirements of GDPR.

4.3 QCS Client Ltd's Approach to GDPR

QCS Client Ltd is required to take a proportionate and appropriate approach to GDPR compliance. QCS Client Ltd understands that not all organisations will need to take the same steps – it will depend on the volume and types of personal data processed by a particular organisation, as well as the processes already in place to protect personal data. We understand that if we process significant volumes of personal data, including **special categories of data**, or have unusual or complicated processes in place in terms of the way we handle personal data, we will consider obtaining legal advice specific to the processing we conduct and the steps we may need to take.

4.4 GDPR does not apply to any personal data held about someone who has died. Both the Access to Medical Reports Act 1988 and the Access to Health Records 1990 will continue to apply.

4.5 QCS Client Ltd's Process for Promoting Compliance

To ensure QCS Client Ltd compliance with GDPR, a suite of documents are available and should be read in conjunction with this overarching policy to provide a framework:

- Initial Privacy Impact Assessment Policy & Procedure
- GDPR – Key Terms Guidance
- GDPR - Key Principles Guidance
- GDPR - Processing Personal Data Guidance
- Appointing a Data Protection Officer Guidance
- Data Security and Retention Policy & Procedure
- Website Privacy Policy & Procedure
- Subject Access Requests Policy & Procedure
- Subject Access Requests Process Map Policy & Procedure
- Subject Access Requests - Request Letter Policy & Procedure
- Rights of a Data Subject Guidance
- Breach Notification Policy & Procedure
- Breach Notification Process Map Policy & Procedure
- Fair Processing Notice Policy & Procedure
- Consent Form
- GDPR - Transfer of Data Guidance
- Privacy Impact Assessment Policy & Procedure

4.6 Overview of Key Principles and Documents

The key principles and themes of each of the documents listed above are summarised below:

Initial Audit and Privacy Impact Assessment

QCS Client Ltd understands that we should conduct an audit of the personal data we currently process. This can be carried out internally by QCS Client Ltd with the assistance of key staff members. The audit will reveal whether the ways in which QCS Client Ltd processes personal data meet the requirements of GDPR and will also indicate whether QCS Client Ltd should delete some of the personal data it currently holds. An initial Privacy Impact Assessment template is provided as part of the GDPR documentation.

Key Terms

GDPR places obligations on all organisations that process personal data about a Data Subject. A brief description of those three key terms is included in the Definitions section of this document and are expanded

upon in the Key Terms Guidance.

The requirements that QCS Client Ltd need to meet vary depending on whether QCS Client Ltd is a Data Controller or a Data Processor. We recognise that in most scenarios, QCS Client Ltd will be a Data Controller. The meaning of Data Controller and Data Processor, together with the roles they play under GDPR, are explained in the Key Terms Guidance.

Special categories of data attract a greater level of protection, and the consequences for breaching GDPR in relation to special categories of data may be more severe than breaches relating to other types of personal data. This information is also covered in more detail in the Key Terms Guidance.

Key Principles

There are 6 key principles of GDPR which QCS Client Ltd must comply with. These 6 principles are very similar to the key principles that were set out in the Data Protection Act 1998. They are:

- Lawful, fair and transparent use of personal data
- Using personal data for the purpose for which it was collected
- Ensuring the personal data is adequate and relevant
- Ensuring the personal data is accurate
- Ensuring the personal data is only retained for as long as it is needed
- Ensuring the personal data is kept safe and secure

These key principles are explained in more detail in the guidance entitled 'GDPR – Key Principles'.

QCS Client Ltd recognises that in addition to complying with the key principles, QCS Client Ltd must be able to provide documentation to the Information Commissioner's Office (ICO) on request, as evidence of compliance. We understand that we must also adopt 'privacy by design'. This means that data protection issues should be considered at the very start of a project, or engagement with a new Service User. Data protection should not be an after-thought. These ideas are also covered in more detail in the Key Principles Guidance.

Processing Personal Data

The position has been improved under GDPR in terms of the ability of care sector organisations to process special categories of data. The provision of health or social care or treatment or the management of health or social care systems and services is now expressly referred to as a reason for which an organisation is entitled to process special categories of data.

In terms of other types of personal data, QCS Client Ltd must only process personal data if it is able to rely on one of a number of grounds set out in GDPR. The grounds which are most commonly relied on are:

- The Data Subject has given his or her consent to the organisation using and processing their personal data
- The organisation is required to process the personal data to perform a contract; and
- The processing is carried out in the legitimate interests of the organisation processing the data – note that this ground does not apply to public authorities

The other grounds which may apply are:

- The processing is necessary to comply with a legal obligation
- The processing is necessary to protect the vital interests of the Data Subject or another living person
- The processing is necessary to perform a task carried out in the public interest

The grounds set out above and the impact of the changes made in respect of special categories of data are explained in more detail in the guidance entitled 'GDPR – Processing Personal Data'.

Data Protection Officers

QCS Client Ltd understands that some organisations will need to appoint a formal Data Protection Officer under GDPR (a "**DPO**"). The DPO benefits from enhanced employment rights and must meet certain criteria, so we recognise that it is important to know whether QCS Client Ltd requires a DPO. This requirement is outlined in the policy and procedure on Data Protection Officers.

Whether or not QCS Client Ltd needs to appoint a formal Data Protection Officer, QCS Client Ltd will appoint a single person to have overall responsibility for the management of personal data and compliance with GDPR.

GDPR01 - Overarching GDPR Policy and Procedure

Data Security and Retention

Two of the key principles of GDPR are data retention and data security.

- Data retention refers to the period for which QCS Client Ltd keeps the personal data that has been provided by a Data Subject. At a high level, QCS Client Ltd must only keep personal data for as long as it needs the personal data
- Data security requires QCS Client Ltd to put in place appropriate measures to keep data secure

These requirements are described in more detail in the policy & procedure entitled Data Security and Retention.

Website Privacy Policy & Procedure

Where QCS Client Ltd collects personal data via a website, we understand that we will need a GDPR compliant website privacy policy. The privacy policy explains how and why personal data is collected, the purposes for which it is used and how long the personal data is kept. A template website policy is provided.

Subject Access Requests

One of the key rights of a Data Subject is to request access to and copies of the personal data held about them by an organisation. Where QCS Client Ltd receives a Subject Access Request, we understand that we will need to respond to the Subject Access Request in accordance with the requirements of GDPR. To help staff at QCS Client Ltd understand what a Subject Access Request is and how they should deal with a Subject Access Request, a Subject Access Request Policy & Procedure is available to staff. A QCS Client Ltd process map to follow when responding to a Subject Access Request, as well as a Subject Access Request letter template is also included.

The Rights of a Data Subject

In addition to the right to place a Subject Access Request, Data Subjects benefit from several other rights, including the right to be forgotten, the right to object to certain types of processing and the right to request that their personal data be corrected by QCS Client Ltd. All rights of the Data Subject are covered in detail in the corresponding guidance.

Breach Notification Under GDPR

We understand, that in certain circumstances, if QCS Client Ltd breaches GDPR, we must notify the ICO and potentially any affected Data Subjects. There are strict timescales in place for making such notifications. A policy and procedure for breach notification that can be circulated to all staff, together with a process map for QCS Client Ltd to follow if a breach of GDPR takes place is available.

We understand that this requirement is likely to have less impact on NHS organisations that are already used to reporting using the NHS reporting tool.

Fair Processing Notice and Consent Form

Organisations are required to provide Data Subjects with certain information about the ways in which their personal data is being processed. The easiest way to provide that information is in a Fair Processing Notice. A Fair Processing Notice template is available for QCS Client Ltd to use and adapt on a case by case basis.

The Fair Processing Notice sits alongside a consent form which can be used to ensure that QCS Client Ltd obtains appropriate consent, particularly from the Service User, to the various ways in which QCS Client Ltd uses the personal data. The Consent Form contains advice and additional steps to take if the Service User is a child or lacks capacity.

Transfer of Data

If QCS Client Ltd wishes to transfer personal data to a third party, we understand that we should put in place an agreement to set out how the third party will use the personal data. The transfer would include, for example, using a data centre in a non-EU country. If that third party is based outside the European Economic Area, we recognise that further protection will need to be put in place and other aspects considered before the transfer takes place. Guidance has been produced to explain the implications of transferring personal data in more detail.

GDPR01 - Overarching GDPR Policy and Procedure

Privacy Impact Assessments

In addition to carrying out an Initial Impact Assessment (referred to above), QCS Client Ltd will carry out further assessments each time it processes personal data in a way that presents a “high risk” for the Data Subject. Examples of when a Privacy Impact Assessment should be conducted are provided in the relevant policy & procedure. Given the volume of special categories of data that are frequently processed by organisations in the health and care sector, there are likely to be a number of scenarios which require a Privacy Impact Assessment to be completed.

The Privacy Impact Assessment template may also be used to record any data protection incidents, such as breaches or 'near misses'.

4.7 Compliance with GDPR

QCS Client Ltd understands that there are two primary reasons to ensure that compliance with GDPR is achieved:

- It promotes high standards of practice and Care, and provides significant benefits for staff and, in particular, Service Users
- Compliance with GDPR is overseen in the UK by the ICO. Under GDPR, the ICO has the ability to issue a fine of up to 20 million Euros (approximately £17,000,000) or 4% of the worldwide turnover of an organisation, whichever is higher. The potential consequences are therefore significant.

QCS Client Ltd appreciates that it is important to remember, however, that the intention of the ICO is to educate and advise, not to punish. The ICO wants organisations to achieve compliance. A one-off, minor breach may not attract the attention of the ICO but if QCS Client Ltd persistently breaches GDPR or commits significant one-off breaches (such as the loss of a large volume of personal data, or the loss of special categories of data), it may be subject to ICO enforcement action. In addition to imposing fines, the ICO also has the power to conduct audits of QCS Client Ltd and our data protection policies and processes. QCS Client Ltd realises that the ICO may also require QCS Client Ltd to stop providing services, or to notify Data Subjects of the breach, delete certain personal data we hold or prohibit certain types of processing.

GDPR01 - Overarching GDPR Policy and Procedure

5. Procedure

5.1 All staff should review the GDPR policies and procedures and guidance that will be produced over the next few months.

5.2 [registered provider] will nominate a person or team to be responsible for data protection and GDPR compliance (if a formal Data Protection Officer is not required, somebody with an understanding of the requirements who can act as a day-to-day point of contact will be chosen).

5.3 Prof Charlie Brown should ensure all staff understand the policies and procedures provided, including how to deal with a Subject Access Request and what to do if a member of staff breaches GDPR.

5.4 Prof Charlie Brown will consider providing training internally about GDPR (in particular, the Key Principles of GDPR) to all staff members.

5.5 QCS Client Ltd will conduct an audit of the personal data currently held by QCS Client Ltd (the initial Privacy Impact Assessment template provided will be used for this purpose).

5.6 QCS Client Ltd will delete any personal data that QCS Client Ltd no longer needs, based on the results of the audit conducted, taking into account any relevant guidance, such as the Records Management Code of Practice for Health and Social Care 2016.

5.7 QCS Client Ltd will, if necessary, put in place new measures or processes to ensure that personal data continues to be processed in line with GDPR.

5.8 QCS Client Ltd will, if necessary, finalise and circulate a Fair Processing Notice to Service Users.

5.9 QCS Client Ltd will ensure proper consent is obtained from each Service User in line with GDPR regulations (the Consent Form provided can be used for this purpose). QCS Client Ltd will review the additional steps that QCS Client Ltd should be taken to ensure that QCS Client Ltd obtains consent from parents, guardians, carers or other representatives where QCS Client Ltd works with children or those who lack capacity.

5.10 QCS Client Ltd will ensure that processes and procedures are in place to respond to requests made by Data Subjects (including Subject Access Requests) and to deal appropriately with any breaches or potential breaches of GDPR.

5.11 Prof Charlie Brown will maintain a log of decisions taken and incidents that occur in respect of the personal data processed by QCS Client Ltd using the QCS Client Ltd Privacy Impact Assessment template.

GDPR01 - Overarching GDPR Policy and Procedure

6. Definitions

6.1 Data Subject

- The individual about whom QCS Client Ltd has collected personal data

6.2 Data Protection Act 2018

- The Data Protection Act 2018 is a United Kingdom Act of Parliament that updates data protection laws in the UK. It sits alongside the General Data Protection Regulation and implements the EU's Law Enforcement Directive

6.3 GDPR

- **General Data Protection Regulation (GDPR)** (EU) 2016/679 is a regulation in EU law on data protection and privacy for all individuals within the European Union. It was adopted on 14 April 2016 and after a two-year trasition period became enforceable on 25 May 2018

6.4 Personal Data

- Any information about a living person including but not limited to names, email addresses, postal addresses, job roles, photographs, CCTV and special categories of data, defined below

6.5 Process or Processing

- Doing anything with personal data, including but not limited to collecting, storing, holding, using, amending or transferring it. You do not need to be doing anything actively with the personal data – at the point you collect it, you are processing it

6.6 Special Categories of Data

- Has an equivalent meaning to “Sensitive Personal Data” under the Data Protection Act 2018. Special Categories of Data include but are not limited to medical and health records (including information collected as a result of providing health care services) and information about a person’s religious beliefs, ethnic origin and race, sexual orientation and political views

Key Facts - Professionals

Professionals providing this service should be aware of the following:

- GPDR provides greater protection for staff and Service Users in respect of their personal data
- Compliance is mandatory, not optional
- QCS Client Ltd has adopted an appropriate and proportionate approach what is right and necessary for QCS Client Ltd may not be right for another organisation
- Achieving compliance with GDPR will not only reduce the risk of ICO enforcement or fines but will also promote a better quality service for Service Users and an improved working environment for staff
- This is the overarching policy and provides a high level reference to all areas that are important for compliance with GDPR
- Undertanding of the content of this policy should be embedded with all staff at QCS Client Ltd
- QCS Client Ltd must appoint a person with overall responsibility for managing GDPR. This person may be an official Data Protection Officer (DPO) or a person appointed to oversee privacy, govenance and data protection

GDPR01 - Overarching GDPR Policy and Procedure

Key Facts - People Affected by The Service

People affected by this service should be aware of the following:

- Your personal data will be protected
- You have a right to see what information we hold about you
- You will be asked for your consent before we obtain your personal data in line with GDPR requirements
- In addition to the GDPR regulations, our staff will continue to follow confidentiality policies in relation to all aspect of your Care

Further Reading

As well as the information in the 'Underpinning Knowledge' section of the review sheet we recommend that you add to your understanding in this policy area by considering the following materials:

The Records Management Code of Practice for Health and Social Care 2016 has been issued by the Information Governance Alliance for the Department of Health. It is available on the NHS Digital website

https://digital.nhs.uk/article/1202/Records-Management-Code-of-Practice-for-Health-and-Social-Care-2016

Outstanding Practice

To be ‘Outstanding’ in this policy area you could provide evidence that:

- QCS Client Ltd provides training to all staff in respect of GDPR and the new policies and processes that have adopted
- QCS Client Ltd conducts Privacy Impact Assessments for each new processing activity carried out, whether or not the processing presents a 'high risk' to the Data Subjects
- There is evidence that QCS Client Ltd conducts regular (6 monthly or annual) audits of the personal data that is processed to ensure continued compliance with GDPR
- QCS Client Ltd can evidence that there are processes in place for ensuring QCS Client Ltd remains up to date with guidelines and recommendations relating to data protection, including ICO guidance and guidance issued by NHS Digital and this information is effectively cascaded to all relevant staff
- The wide understanding of the policy is enabled by proactive use of the QCS App

GDPR01 - Overarching GDPR Policy and Procedure

This page is deliberately left blank