CareQuality Commission

QUICK GUIDE

Information Security

This leaflet defines information security and governance and provides summarised advice from the CQC Information Security and Governance Policy document. It has been produced as a quick reference guide and contains the top ten good practice pointers to assist staff in their day to day business activities.

Information is an asset within CQC which, like other important assets, has value to our business activities and consequently needs to be appropriately protected.

Information security measures are designed to protect information from a wide range of threats in order to ensure that our information is appropriately secure, accurate and available when we need it. This can be summarised as:

Confidentiality	Ensuring only those who ought to have access can do so
Integrity	Ensuring that information cannot be modified without detection
Availability	Ensuring that information can be accessed when needed

Information can exist in many forms. It can be printed, handwritten, stored electronically or as digital images. The information may be transmitted by post or electronically.

Information security is achieved by implementing a suitable suite of controls, which include policies, practices, procedures, organisational structures and software/technical controls.

Some aspects of information security and governance are contained within legislation. The most notable UK Acts are:

- **Data Protection Act**
- **Computer Misuse Act**
- **Freedom of Information Act**
- **Public Records Act**

Additionally, staff are under a common law obligation to preserve the confidentiality of service user information.

Information security will only be successful with the active participation of all staff.

More detailed information can be found on the intranet - see **Directorates and Teams > Governance & Legal Services > Information Security**

Good Practice 'Top 10'

Passwords

Ensure that you change your passwords regularly (the applications will prompt you) and use strong passwords with at least 8 characters and a combination of at least 3 of the following; lower case, upper case, numbers and special characters.

Passes

Wear your CQC pass visibly in our offices and ensure that you take them off when you leave the building. Do not let people tailgate you into our access controlled areas and challenge anyone who tries to do so.

Training

Completion of IG and Security training is an annual requirement mandated by the Cabinet Office. Please take the time to complete the training package on the Marton House website as soon as possible during each financial year.

Homeworking and Travel

The same security measures apply when you are working at home or on the move to those required in the office. Additionally, CQC assets, both electronic and hard copy, should be safeguarded when in transit and whilst in your home environment.

Email and Encryption

Personal and sensitive information should not be contained within the body of emails being sent outside of the CQC trusted network. If you do need to send this kind of information outside CQC ensure that it is encrypted within an attachment.

Social Media

Social media is a useful communications tool used increasingly by CQC. Unauthorised personal use of social media should not contain CQC information whether considered sensitive or not.

Unsolicited Communications

It is common to receive emails and calls from unknown sources or sales representatives. These may also include attempts to get you to reveal corporate or personal information (phishing). If you receive such communications do not reply - simply delete the email and report the matter to the security mailbox. However, if you think the request may be a legitimate request for information, please forward it to information.access@cqc.org.uk immediately.

Clear Desks

All documents containing personal and sensitive information should be locked away outside normal business hours. Computers should be shut down at the end of the working day and have the screen lock applied (Ctr, Alt & Del, then hit 'Enter') if you are going away from your desk for lunch or a meeting.

Retention, Disposal and Destruction

Retention periods for data in CQC has been defined in the schedule published on the intranet by the Knowledge and Information Management team. Once data is no longer required it should be destroyed securely in line with CQC Information Security and Governance Policy available on the intranet.

Incident Reporting

In the event that something does go wrong, or you suspect that there may have been a data breach, please report it to the security mailbox: security@cqc.org.uk

If you have any questions about anything in this leaflet or the wider Information Security Policy and Procedures, please contact security@cqc.org.uk or the Information Security Manager (Derek.wilkinson@cqc.org.uk) directly.