CQC Information Classification Scheme

In line with recent changes to the Government classification scheme, CQC have adopted the new guidelines along with all other public bodies.

The previous protective markings of 'Protect' and 'Restrict' should no longer be in use within the public sector. They have been replaced with a single protective marking of 'Official' which covers all information stored and processed by public bodies including CQC. In order to delineate between information which we may want to make public or publish on our website and that which we may want to apply other security controls to, CQC intend to use 'Official' for all information which is not deemed to require any specific protection and 'Official Sensitive' for that which needs additional protective measures to be applied.

There is no requirement to protectively mark any documents which fall in the Official category. However, documents protectively marked as 'Official Sensitive', both hard copy and electronic, should be clearly labelled as such in the header and footer section of the document. Additionally, all emails containing official sensitive information should have the marking 'OFFICIAL SENSITIVE' in the subject field.

Decisions on the protective marking to be applied to documents are the responsibility of the originator. However, as a guide, if the document contains confidential personal information which can be used to identify an individual and provides additional information about their health status, financial details or other information which they could reasonably expect to be kept confidential then that document should be marked as official sensitive.

Classification Descriptions

Security Classification	Description
OFFICIAL	All information processed within CQC is deemed to be classified as 'Official' regardless of the associated sensitivity.
OFFICIAL - SENSITIVE	Information which is deemed to be sensitive and is not intended to be released outside of the organisation without a specific business reason and authorisation. This may be personally sensitive information relating to individuals (e.g. health information) or business sensitive information such as operational plans or financial forecasts which have not been authorised for publication or release to the general public.

Handling Guidance

Official

There is no requirement to mark documents or emails which are classified Official. Advice should be sought prior to releasing Official information outside of CQC, this can be done via the Information Rights, Records and Document Management or Information security team.

During the normal course of business activities it is necessary to write to, including email, people outside of CQC. This will, by definition, contain Official information. Individual members of staff should exercise judgement as to whether or not there is a need for the recipient to view such information and whether this information is being sent directly to the intended recipient. If the address being used is a general one and not direct to the named individual, then there may still be a need for this information to be password protected.

Official Sensitive

Greater care should be exercised over the use, transmission and storage of Official Sensitive information.

In general this category of information should only be used when it is strictly necessary to include personal data in documents and correspondence. Staff should also ensure that they consider whether communicating Official Sensitive information is necessary or whether the use of anonymised information will suffice.

Identification of Official Sensitive information

Official Sensitive documents are defined as containing either personally sensitive information relating to individuals or business sensitive information.

Personally sensitive information refers to documents which may identify an individual and contain details of their health status, financial situation or other confidential information which they may not want to be made public.

Examples of documents that may contain personally sensitive information would include:

- Notifications
- Whistleblowing enquiries
- Safeguarding correspondence
- Human resources employee records

Business sensitive information refers to documents that contain information relating to the organisation that is not made available to the public and that could negatively affect the operation of the organisation if released.

Examples of documents that may contain business sensitive information would include:

- Contracts or Tenders with 3rd party suppliers,
- Documents relating to the financial affairs of a provider.

Identification of persons

The information which can be used to identify an individual is quite broad and a person would be considered identifiable if any separate pieces of information can be used in conjunction with others provided (or already known) to accurately identify a single individual.

The following list of characteristics could be used either individually or together to identify a specific person:

- Initials
- First Name
- Surname
- Job Title
- Residential Address
- Group Membership
- Employer Address
- Employer details
- Age or Date of Birth
- Gender
- Physical Characteristics

Therefore if this information was received along with information an individual would not want disclosed this would automatically be categorised as **Official Sensitive**.

Confidential Personal Information

Any information which an individual may not want known to individuals who do not require the information for legitimate reasons

The following list of characteristics could be regarded by an individual as private:

- Political beliefs
- Religion
- Sexual orientation
- Union membership
- Personal address

- Personal telephone number
- Health details
- Employment details/history
- Victimisation incidents (i.e. the victim)
- Alleged abuse incidents (i.e. the perpetrator)
- Criminal accusations/convictions

Storage and Access

CRM:

Because CRM is a restricted system and all CQC employees with access to CRM have been security checked and allocated with a restricted password, there is no need to restrict access to individual documents. Employees will be given appropriate access to CRM, dependent on their role, and will therefore only be able to view documents that are relevant to their specific job role.

It has been deemed that employees can access all documents within the areas of CRM that they have been granted access permissions to view. Viewing of these documents, however, should be done with discretion and only when there is a business need to do so.

Y: Drive:

Within the Y: Drive, as with CRM, employees are granted access to specific folders depending on the requirement for access. This is, again, determined by the specific job role of the individual employee.

There is, therefore, no requirement, as a matter of course, to restrict individual documents within the Y: Drive folders.

Documents must still be stored, however, in line with the existing RDM policy and processes, which can be found on the Intranet.

Sharing

There is no requirement to apply protective measures when sharing Official documents via post, verbally, via fax, or e-mail correspondence.

The following protective measures should be applied to the transmission Official Sensitive data:

- All emails should have the marking ‘OFFICIAL SENSITIVE’ in the subject field.
- Documents sent externally should be sent as an encrypted file using Winzip.

- Paper documents should only be sent via Special Delivery or by using a secure point to point, same day courier. If Sensitive paper documentation is carried by a staff member during travel it should be kept secured and never left unattended.
- Discretion should be used when discussing any Official Sensitive information, to ensure that the conversation cannot be overheard by unauthorised individuals.
- Official Sensitive information should not be sent via fax if it can be sent by other means. This is to negate the risk of the information being sent to an unattended or public fax machine or to the wrong place entirely. If the use of a fax is unavoidable then users should refer to the Safe Haven process (details can be found on the intranet).

Redacting

If the sensitive content of the document can be removed; and thus reduce the security level from Official Sensitive to Official then the document can be managed as an Official document.

For further details on redaction processes please contact the Records and Document Management (RDM) team by e-mailing RDM.Helpdesk@cqc.org.uk.

Exceptions

There may be cases where particularly sensitive categories of information fall outside the guidelines included in this document e.g. provider financial information. If there is any doubt over the classification of documents or information then advice should be sought from the Information Security or RDM teams.

Reporting Incidents

If you become aware of any incident whereby the above guidance is not followed, please report this to your line manager and Security@CQC.org.uk as soon as possible.