

CJSM Usage Guidelines

Criminal Justice Secure eMail (CJSM) is intended to provide a secure way for criminal justice agencies and practitioners to exchange emails with each other.

As a general rule, you should only use CJSM for legitimate business purposes relating to the Criminal Justice System. However, you can use CJSM for day to day communications with organisations that you regularly pass sensitive emails to.

You or your organisation could have your CJSM account suspended or removed if:

- You share your user account details or CJSM password with anyone else. Secretaries, PA's and clerks may be allowed to use the details on a user's behalf, but the user will remain responsible for what they do with it.
- You allow strangers to enter areas of your premises where IT systems with access to CJSM are in use. Where this is unavoidable, all visitors must be escorted at all times.
- You send confidential information to people who don't need to know it.

Email Content

There are times when criminal justice agencies and practitioners need to send emails containing material that, out of context, might be considered illegal (e.g. racist, sexist, pornographic, defamatory or threatening material) or otherwise unacceptable (e.g. malicious language designed to offend), such as statements contained within a case file.

Consequently, there are no restrictions on the type of information that can be sent by CJSM, other than a general requirement that it must be acceptable within the context and purpose for which it is being sent.

CJSM must not be used to send information with a sensitivity level higher than RESTRICTED, as defined by the Government Protective Marking Scheme.

We will develop more detailed guidance on how such information should be classified as more people and organisations start to use CJSM.

Protective Marking and Special Handling Instructions

The Government Protective Marking Scheme has been adopted by several criminal justice organizations. However, users don't have to adopt it to use CJSM.

Criminal justice agencies that have adopted the Government Protective Marking Scheme, may use CJSM to send emails and attachments with any of the following markings:

- NOT PROTECTIVELY MARKED
- RESTRICTED (with or without allowed special handling descriptors such as COMMERCIAL or MANAGEMENT)
- PRIVATE
- and/or special caveat markings, such as EYES ONLY

Even if they have not adopted the Government Protective Marking Scheme, criminal justice agencies or practitioners may still use these markings (apart from RESTRICTED) when sending emails and attachments by CJSM.

They may also use other markings that suggest that information being sent needs to be handled carefully.

CJSM users receiving protectively marked emails or attachments must comply with any such handling requirements. Where handling requirements are not clear, the sender should be consulted.

Unless a message or attachment is specifically marked as NOT PROTECTIVELY MARKED, it must be protected by CJSM users, in accordance with the requirements set out in CJSM's Terms and Conditions. It is the user's responsibility to decide whether an email or its attachments needs special handling over and above the minimum requirements set out in the Terms and Conditions.

Regulatory and Statutory Issues

CJSM users must comply with all relevant current regulatory and statutory requirements, in particular those relating to allowable email content, including:

- the Data Protection Act 1998
- the Computer Misuse Act 1990
- the Freedom of Information Act 2000
- the Police and Criminal Evidence Act 1998
- the Regulation of Investigatory Powers Act 2000

Need to Know

CJSM users must make sure that they only send sensitive information to those who have a need to know it, and are authorised to do so. If there is any doubt, then the recipient organisation should be consulted.

Signature Block

CJSM users must insert a signature text block in all outgoing email messages giving the recipient enough information to telephone or email the sender if there is a problem with the received message.

Confidentiality Statement

It is recommended that any emails sent by CJSM which contain sensitive information should include a confidentiality statement, possibly included within the signature block.

Organisations may decide their own wording for such a statement, but here is an example:

"The information contained in this message is confidential. It is intended solely for the use of the individual or entity to whom it is addressed and others authorised to receive it who have a 'need to know'. If you are not the intended recipient, you are hereby notified that any use, copying, dissemination or disclosure of this information is strictly prohibited and may be unlawful. If you have received this communication in error, please return it to the sender."

Falsely claiming emails have not been received

CJSM users must not falsely claim that they haven't received emails sent by CJSM.

It is the responsibility of the sender to request delivery receipts or read receipts, as required.

Disclosure of Information

CJSM users must not forward any email or its attachments to anyone who is not a CJSM user, unless:

- the email and/or attachment is either explicitly marked NOT PROTECTIVELY MARKED or the user is otherwise certain that the material is not sensitive; or
- the recipient(s) can be trusted to handle the material securely according to its sensitivity and forwarding is by a suitably secure communication channel.

Information Integrity

CJSM users must not modify, extract or selectively forward the contents of any email without specifying that they have done so.

Multiple Log-on

Mailbox users must not connect or try to connect to their CJSM account from different computers at the same time.

Technical Requirements

Users must let the CJSM Helpdesk know if there is any significant change to their technical infrastructure which does or might affect access to, or the integrity of, the CJSM service. If such a change is reported, OCJR may carry out an impact assessment to see what, if any, affect these changes may have.

Users must make regular back-ups of data to minimise any interruption to the criminal justice process in the event of technical problems.

Users must have secure data storage facilities and their data archiving and retention policies must be consistent with the nature of the data stored, and consistent with the needs of the criminal justice system. Where "Restricted" data is to be deleted, the same standards of security must be applied to its disposal.

Where multiple users have access to an organisation's CJSM account, the organisation must ensure that all systems used for sending and receiving messages by CJSM are secure.

<https://www.cjsm.net/HelpSecureEmailExternal.do;jsessionid=59AF6639D236860D8AD3095820584ADE>