



## Terms & Conditions for Connection to the Criminal Justice Secure eMail Service (CJSM)

This version (8.5M L) for completion by organisations,  
including sole practitioners with staff

---

1. We will ensure that all users in our organisation comply with UK Data Protection and Privacy Laws and all professional codes of conduct under which we are bound and all information transmitted through CJSM is treated as 'Restricted'. We acknowledge that any breach of these provisions may result in access to CJSM being suspended or terminated.
2. We agree to ensure that all members and employees of our organisation who are given accounts on, or authorised access to, the CJSM understand the conditions on which connection has been granted as set out in this document and that the conditions are ongoing and cover any continuous use of CJSM. To this end:
  - all those users given accounts will sign a commitment to adhere to the Terms and Conditions.
3. To enable the source of any causes of security breaches to be traced for SMTP users, we confirm that we will maintain accurate and up to date records/logs of use showing who has accessed CJSM via SMTP for a rolling period of 6 months.
4. In the event of a security breach, or suspected breach of security, within our environment and involving Justice Data or our access to the CJSM, we will inform the CJSM Administrators immediately (via the CJSM Helpdesk). We understand that the MOJ reserves the right to investigate security incidents and we confirm that, should such an investigation be necessary, we will provide any necessary support, which may include the supply of relevant logs, to the best of our ability.
5. We will communicate to the MOJ (via the CJSM Helpdesk) all significant changes to the organisation's technical infrastructure that impact access to, or could impact the integrity of, the CJSM service so that an assessment can be undertaken.
6. We confirm that all users of our organisation's IT systems (including, where relevant, contractors and third party users):
  - are authorised users and can be individually identified by having unique user names, email addresses and passwords (passwords must be a minimum of 8 alphanumeric characters and changed at least every 90 days); i.e. passwords must be a mix of upper and lower case alphabetic characters plus numeric and/or special characters.
  - will not share their user credentials, and that if any user credential is compromised it will be changed as soon as possible and that users will be prevented from having multiple concurrent email sessions;
  - receive appropriate security awareness training and awareness updates in organisational policies and procedures as relevant for their role.
7. We will not transmit information through the CJSM that we know, suspect or have been advised is of a higher level of sensitivity than the CJSM is designed to carry (that is 'Restricted' material) nor will material be forwarded to anybody other than on a strict need to know basis.
8. We will not use CJSM for system to system automated emails without the permission of the MOJ.
9. We confirm that our organisation has a business continuity/disaster recovery plan in place to minimise any interruption to the Justice process in the event of a loss of IT capability.
10. We confirm that our organisation has secure data storage facilities; and that our data archiving and retention policies are consistent with the nature of the data stored, and consistent with the needs of the Justice System. We further confirm that, where 'Restricted'<sup>1</sup> data is to be deleted, the same standards of security are applied to its disposal.

---

\* 'Restricted' information, for the purpose of this agreement, is defined as Justice sensitive business information (that may or may not bear the Government Protective marking RESTRICTED or PROTECT), the unauthorised disclosure of which would :- cause substantial distress to individuals; prejudice the investigation or facilitate the commission of crime; breach proper undertakings to maintain the confidence of information provided by third parties or undermine the proper management of the public sector and its operations

---

**All contact with the MOJ to be made through:**

The CJSM Administrators

C&WW (for the MOJ), 76 Hammersmith Road, London , W14 8UD

Telephone via the CJSM Helpdesk 0870 010 8535





11. We confirm that we have carried out a business-focused risk assessment of our computer systems as appropriate to our organisation and will carry out regular reviews/audits of the IT infrastructure e.g. to ISO27002 (ISO17799) or similarly appropriate standards. If an assessment has not already taken place, we plan to complete one and implement recommendations within the next six months.
12. We confirm that our organisation prevents strangers and unauthorised personnel from entering areas of its premises where IT systems that have access to the CJSM or information transmitted via the CJSM are in use. Where this is not possible, all visitors are escorted at all times.
13. We confirm that all portable computers and devices, e.g. USB flash drives, that will be used for sending/receiving CJSM email or for storing 'Restricted' data are appropriately protected against unauthorised use and that data is encrypted to safeguard against unauthorised disclosure.
14. We will ensure that information transmitted to/from CJSM is only transmitted between systems within this organisation that we believe to be secure.
15. We will inform the MOJ before accessing CJSM if any part of our network is outside the UK. This includes offshore network maintenance and any remote access from outside the UK. We also undertake to inform the MOJ if we plan to move any part of our network outside of the UK.
16. We confirm all wireless installation over which CJSM is intended to be used will be secured to WPA/WPA2/WPA 2 Enterprise standards and is supplied by a known and trusted source (i.e. not a hotel, café or other hotspot). Any other proposed installation of WiFi will be agreed with MOJ prior to use.
17. We understand that authorisation to use a Tablet Computer, smartphone or other wireless device has to be obtained from the MOJ before they can be used on CJSM and that only HMG accredited systems/ MOJ approved devices will be accepted.
18. We confirm that a firewall is used to protect our systems/organisation connecting to CJSM and that it is frequently monitored, maintained and not disabled.
19. We confirm that all machines used to access the CJSM prevent malicious software by running up-to-date Anti-virus and Spyware packages with regular and frequent updates being applied.
20. We confirm that operating system updates and security patches are regularly applied to all servers used to access the CJSM and all client machines within the organisation.
21. We confirm that we will only connect to CJSM from within the UK.
22. We note that government organisations that have .gsi.gov.uk, .gsx.gov.uk or .pnn.police.uk or similar email addresses are likely to submit their emails to audit procedures as part of normal HM Government policy and that any such monitoring would include any emails that may be sent to them via the CJSM.
23. We confirm CJSM will not be used for the purposes of spamming or advertising. We accept that should we use CJSM in this way we will be immediately disconnected from the service.
24. We note that the MOJ reserves the right to audit our access to CJSM and our compliance with the above Terms and Conditions and we confirm that we will cooperate with the auditors and audit process. We also note that the MOJ would provide at least 4 weeks notice of any such audit.

Signature \_\_\_\_\_ Name (please print) \_\_\_\_\_ Date \_\_\_\_\_ Position \_\_\_\_\_

On behalf of  
**(Organisation name)** \_\_\_\_\_

