Terms & Conditions for Connection to the
Criminal Justice Secure eMail Service (CJSM)
This version (9.6) for completion by organisations,
including sole practitioners with staff

CJSM is supplied to the organisation in accordance with the following Terms & Conditions, and associated User Terms & Conditions. **All organisations local user representatives' must read and acknowledge their understanding and agreement to the following:-**

1. We will ensure that all users in our organisation comply with the UK Data Protection Act 1998, relevant privacy regulations and all professional codes of conduct under which we are bound. Furthermore, information transmitted through CJSM is treated as either :-

    a. Within the 'OFFICIAL[1]' tier of the Government Security Classifications (GSC), where the sensitivity attached to said information is such that transmission using the Internet (without additional assured protection) is not appropriate and/or

    b. Information at RESTRICTED[2] and below for information marked with the GPMS.

    We acknowledge that any breach of these provisions may result in access to CJSM being suspended or terminated.

2. In addition to the above, we will ensure that our users are made aware of the need to comply with any handling instructions related to the information communicated via CJSM, particularly where this relates to the onward transmission or storage of said data. Furthermore, we will ensure that any data that is communicated via CJSM will be accompanied by handling instructions where appropriate.

3. 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.

4. 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.

5. In the event of a security breach, or suspected breach of security within our environment and involving CJSM originated 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.

6. 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. Furthermore, any 'Cloud' service or virtual/shared infrastructure that we migrate our system hosting CJSM to must follow the cloud hosting application process (CHAP).

---

[1] *The majority of information that is created or processed by the public sector is classed as 'OFFICIAL'. This includes routine business operations and services, some of which could have damaging consequences if lost, stolen or published in the media, but are not subject to a heightened threat profile.*

[2] '*Restricted' information, for the purpose of this agreement, is defined as personal and sensitive information (that may or may not bear the Government Protective marking RESTRICTED), 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, Egress Software Technologies Ltd, Unit 16 Quadrant Business Centre,
135 Salusbury Road, London, NW6 6RJ
Telephone via the CJSM Helpdesk 0870 010 8535/ 020 7604 5598

7. 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 9 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/passwords, and that if any user credential/password 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.

8. 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 'OFFICIAL' material) nor will material be forwarded to anybody other than on a strict need to know basis.
9. We will not use CJSM for system to system automated emails without the permission of the MOJ.
10. We confirm that our organisation has a business continuity/disaster recovery plan in place to minimise any interruption to the business in the event of a loss of IT capability.
11. 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 'CJSM originated' data is to be deleted, the same standards of security are applied to its disposal.
12. 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 to the most recent version of ISO270001. If an assessment has not already taken place, we plan to complete one and implement recommendations within the next six months.
13. We confirm that our organisation prevents 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.
14. We will only allow access to the Service from dedicated/official systems used for the purpose of our business. Where this is not possible we will ensure that users only access the CJSM Service from a device which meets these Ts&Cs and has dedicated password protected profiles.
15. We confirm that all devices including portable storage and mobile devices, that will be used for sending/receiving CJSM email or for storing CJSM originated data are protected against unauthorised use; and that data is encrypted to safeguard against unauthorised disclosure through the use of full disk/device encryption to standards acknowledged by the HMG Security Policy Framework (SPF) or the Information Commissioners Office (ICO) (e.g. CAPS or FIPS 140-2[1]).
16. We will ensure that information transmitted to/from CJSM is only transmitted between systems within our organisation that we believe to be secure.
17. 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.

[1] The ***Federal Information Processing Standard*** (**FIPS**) Publication 140-2, (FIPS PUB 140-2),is a U.S. government computer security standard used to accredit cryptographic modules.

Return Address:
The CJSM Administrators, Egress Software Technologies Ltd, Unit 16 Quadrant Business Centre,
135 Salusbury Road, London, NW6 6RJ
Telephone via the CJSM Helpdesk 0870 010 8535/ 020 7604 5598

18. We confirm all wireless installations over which CJSM is intended to be used will be secured to WPA/WPA 2 Enterprise standards and is a home (known and owned) or work network.

19. **We understand that Tablet Computers, Smart Phones or other mobile devices must comply with the CJSM Mobile Device Policy and authorisation has to be obtained from the MOJ before they can be used on CJSM.**

20. 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.

21. 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.

22. 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.

23. We note any emails sent to government organisations via CJSM are likely to be submitted to audit procedures as part of normal HM Government policy.

24. 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.

25. 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 will provide at least 4 weeks notice of any such audit.

26. We understand that the MoJ reserves the right to terminate our connection to CJSM in the event that the above mentioned audit activity reveals significant shortfalls in good security practice (as specified within this document). Similarly, we understand that if the output of the audit activity points to remedial activity being required and we do not demonstrate progress in line with MoJ requirements, our connection with CJSM may be terminated.

27. We confirm that should we become aware of any vulnerabilities to the CJSM I will raise it to the Ministry of Justice immediately.

Declaration:

As the local user representative I am fully aware of my responsibilities in relation to the connection to and use of the CJSM Service as set out in these Terms & Conditions and I am authorised to sign these terms and conditions on behalf of my organisation.

Signature	Name (please print)	Date	Position

On behalf of
(Organisation name) _____

_____

Return Address:
The CJSM Administrators, Egress Software Technologies Ltd, Unit 16 Quadrant Business Centre,
135 Salusbury Road, London, NW6 6RJ
Telephone via the CJSM Helpdesk 0870 010 8535/ 020 7604 5598