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

This version (10.2) for completion by organisations, including sole practitioners with staff

Introduction

The Criminal Justice Secure Mail service (hereafter referred to as 'CJSM') is owned by the Ministry of Justice (hereafter referred to as 'MoJ') and run by Egress Software Technologies Limited (hereafter referred to as 'Egress') on behalf of the MOJ. This document details the Terms and Conditions of service to organisations and individuals which must be accepted and adhered to at all times. It also provides UK Data Protection Act 2018 and EU General Data Protection Regulation (GDPR) baseline information and high-level security details that ensure data processed through and stored on the service remains secure.

Data Protection Baseline

The MoJ is the data controller for personal data processed and stored on CJSM for the purpose of delivering and managing the service.

Egress as an approved government supplier collects and processes personal data for purposes of the administration of the CJSM Service; Egress are Data Processors on behalf of the MoJ.

Organisations (you) are Data Controllers for the personal data contained within email transaction made under your user accounts on CJSM.

It is for the end user/organisation to satisfy itself that the information transacted over CJSM (by said user) is:

a. lawful in nature,
b. specific in its purpose,
c. adequate and limited to what is necessary
d. accurate
e. processed for no longer than is necessary to its purpose
f. appropriately secure in context with the parameters offered under CJSM.

We collect information about you in accordance with our Privacy Notice and our Cookies Statement. These are available on the CJSM Website.

CJSM Security Controls

CJSM employs the following security controls to ensure the security of personal data under its controls and that transiting the service:

a. Authentication controls to provide assurance that only authorised users have access.
b. Encryption of data in transit to protect personal data being transmitted over the Internet
c. Encryption of data at rest to protect personal data held in CJSM data stores.
d. Network security controls to protect the CJSM from attacks by unauthorised users.
e. Protective Monitoring and auditing across the service to identify and investigate security incidents.

Terms & Conditions

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 2018, the EU General Data Protection Regulation (GDPR) and all professional codes of conduct under which we are bound. Furthermore, we understand that information transmitted through CJSM is classified as OFFICIAL as defined in the Government Security Classifications (GSC) Policy, where the sensitivity attached to said information is such that transmission using the Internet without additional assured protection is not appropriate.

   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 T&Cs.
4. To enable the source of any causes of security breaches to be traced for SMTP, O365 and GSuite users, we confirm that we will maintain accurate and up to date records/logs of use showing who has accessed CJSM for a rolling period of 6 months.
5. In the event of a security breach or suspected breach our environment and involving CJSM originated Data, or our access to the CJSM, we will inform the CJSM Helpdesk immediately. We understand that the MoJ reserves the right to investigate these incidents and we confirm that, should such an investigation be necessary, we will provide any requested 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).
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 in accordance with NCSC's password guidance[i] or must be a minimum of 8 alphanumeric characters and changed at least every 90 days and 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 or destroyed, this is done securely.
12. We understand that CJSM shall not be used as a persistent store, data repository archive capability for email records; and any correspondence or associated material will be removed to a separate system for any retention requirements.
13. We confirm that the 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 National Cyber Security Centre (NCSC) '10 Steps to Cyber Security[ii]. If an assessment has not already taken place, we plan to complete one and implement recommendations within the next six months.
14. 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.

15. 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 T&Cs.
16. 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 and guidance from the NCSC or the Information Commissioners Office (ICO) (e.g. CAPS or FIPS 140-2 1[iii]).
17. We will ensure that information transmitted to/from CJSM is only transmitted between systems within our organisation that we believe to be secure.
18. 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.
19. We confirm all wireless installations over which CJSM is intended to be used will be secured to WPA/WPA 2 or Enterprise standards and is a home (known and owned) or work network.
20. We confirm that all Tablet Computers, Smart Phones or mobile devices used to access CJSM have NCSC's Keeping your smartphones (and tablets) safe guidance[iv] controls (including personal devices, if relevant).
21. We confirm that a firewall is used to protect our systems/organisation connecting to CJSM and that it is frequently monitored and maintained and is not disabled.
22. We confirm that all machines used to access the CJSM prevent malicious software by running up-to-date Anti-virus and Spyware packages with frequent updates being applied.
23. 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.
24. 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.
25. 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.
26. We note that the MoJ reserves the right to audit our access to CJSM and our compliance with the above T&Cs 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.
27. 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.
28. We confirm that should we become aware of any vulnerabilities to the CJSM we will raise it to the MoJ immediately (via the CJSM Helpdesk).

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

Organisation name:

[i] NCSC, Password Guidance: Simplifying your approach, available from: https://www.ncsc.gov.uk/guidance/password-guidance-simplifying-your-approach

[ii] NCSC '10 Steps to Cyber Security, available from: https://www.ncsc.gov.uk/guidance/10-steps-cyber-security

[iii] 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.

[iv] NCSC, Keeping your smartphones (and tablets) safe, available from: https://www.ncsc.gov.uk/guidance/keeping-your-smartphones-and-tablets-safe

Return Address:

Please sign up to these T&Cs using the CJSM Portal.
If necessary, you can sign and email a copy to the CJSM Helpdesk at cjsm.helpdesk@egress.com.