Terms & Conditions for connection to the Criminal Justice Secure Mail Service (CJSM)

This version (10.1) is to be followed by all users

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

The CJSM is supplied to the user in accordance with the following Terms & Conditions. Users understand that continued use of the Service will be taken as their acceptance of these Terms & Conditions and that they are fully aware of their responsibilities in relation to the use of the Service as set out below.

1. I will ensure that I comply with the UK Data Protection Act 2018 and EU General Data Protection Regulation (GDPR), relevant privacy regulations and all professional codes of conduct under which I am bound; furthermore, I 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.

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

2. In addition to the above, I am 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, I will ensure that any data that is communicated via CJSM will be accompanied by handling instructions where appropriate
3. I will control access by others to CJSM data so that only authorised individuals may view such data. I will seek to prevent inadvertent disclosure of sensitive or classified information by avoiding being overlooked when working, also by taking care when printing information received via the CJSM (e.g. by collecting printouts immediately when they are printed, checking that there is no interleaving of printouts, etc.);
4. I agree to be responsible for any use of the CJSM using my unique user credentials (user ID and password, access token or other mechanism as provided/used by me) and e-mail address. As such, I understand that:
    - Passwords must be in accordance with NCSC's password guidance[i] or 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.
    - I must protect my CJSM credentials (username, password etc) for access to the CJSM service. I understand that I may be held liable for any compromise or abuse of the credentials where I have not protected them accordingly.
    - Any actual or suspected disclosure of this information must be reported to the CJSM Helpdesk.
    - I will not use any other user's credentials to access CJSM.
5. I will ensure that computing devices, including mobile devices will not be left unattended unless they are physically secure and require a password for access (a password protected screen saver for instance). Where my/another organisation has implemented other measures to prevent unauthorised viewing of information displayed on IT systems (such as an inactivity timeout that causes the screen to be blanked or to display a screensaver or similar, requiring a user logon for reactivation), I will not attempt to disable such protection.
6. I 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 encryption to standards and guidance from the National Cyber Security Centre (NCSC) or the Information Commissioners Office (ICO) (e.g. CAPS or FIPS 140-2[ii]).
7. I will take precautions to protect all computer media and devices, including mobile devices when carrying them outside my organisation's premises (e.g. not leaving a laptop unattended or on display in a car such that it would encourage an opportunist thief).
8. I will not attempt to make changes to the CJSM for example by adding additional software.
9. I will not transmit information through the CJSM that I know, suspect or have been advised is of a higher level of sensitivity than the CJSM is designed to carry (as per requirement 1 above) nor will material be forwarded to anybody other than on a need to know basis.
10. I will always check that the recipients of e-mail messages are correct so that potentially sensitive information is not accidentally released to any third party; and will disclose information received via the CJSM only on a 'need to know' basis. Furthermore, I will not forward or disclose any sensitive material received via the CJSM unless the recipient(s) can be trusted to handle the material securely according to its sensitivity.
11. I will confirm that I make regular backups-ups of data to minimise an interruption to the justice process in the event of a loss of IT capability.
12. I can confirm that I have secure data storage facilities; and that my data archiving and retention policies are consistent with the nature of the data stored, and consistent with the needs of the justice system. I further confirm that, where CJSM originated data is to be deleted, the same standards of security are

applied to its disposal.

13. I 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.
14. I confirm that I prevent unauthorised personnel from entering areas of my premises where IT systems that have access to the CJSM are in use. Where this is not possible, all visitors are escorted at all times.
15. I will only access the Service from dedicated/official systems used for the purpose of my business. Where this is not possible I will ensure that I only access the CJSM Service from a device which meets these T&Cs.
16. I confirm that all Tablet Computer, Smart Phones or mobile devices used to access CJSM have the NCSC Keeping your smartphones (and tablets) safe guidance[iii] controls in place (including where relevant personal devices).
17. I confirm that a firewall is being used to protect my IT system(s) and that it is frequently monitored, maintained and not disabled.
18. I confirm that any systems/mobile devices used to access the CJSM service prevent malicious software by running up-to-date Anti-virus and Spyware packages as a minimum and that regular and frequent updates are applied to malicious software control.
19. I confirm that operating system updates and security patches are regularly applied to the system used to access the CJSM.
20. I will not attempt to bypass or subvert system security controls or to use them for any purpose other than that intended;
21. I will not attempt to exceed my level of granted access on the CJSM platform.
22. With the exception of my organisation's approved Cloud Service connection (Microsoft Office365, Google G Suite etc). I will not attempt to configure any form of 'web based' mail service/client to send or receive mail from the CJSM service.
23. I confirm any wireless installation over which CJSM is intended to be used will be secured to WPA/WPA 2 or Enterprise standards and is either a home (known and owned) or work network.
24. I confirm CJSM will not be used for the purposes of spamming or advertising. I accept that should I use CJSM in this way I will be immediately disconnected from the service.
25. I understand that my use of any asset which has any intent to damage the confidentiality, integrity or availability of the Service, is automatically deemed unauthorised.
26. I confirm that I will only access the CJSM service from a location that is outside the UK only if authorised by the MoJ (via CJSM Helpdesk).
27. I note that any emails sent to HM Government via CJSM are likely to be submitted to audit procedures as part of normal HM Government policy.
28. I note that the MoJ reserves the right to audit my access to CJSM and my compliance with the above Terms and Conditions and I confirm that I will cooperate with the auditors and audit process. I also not that the MoJ will provide at least 4 weeks' notice of any such audit (where appropriate). Furthermore, I understand that the Service may be subject to monitoring and action taken if any suspected unauthorised misuse identified.
29. I understand that the MoJ reserves the right to terminate my 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, I understand that if the output of the audit activity points to remedial activity being required and I do not demonstrate progress in line with MoJ requirements, my connection with CJSM may be terminated.
30. In the event of a breach of security, or suspected breach of security, within my environment and involving CJSM originated data or my access to the CJSM, I will inform the CJSM Administrators immediately (via the CJSM Helpdesk). I understand that the MoJ reserves the right to investigate security incidents and confirm that, should such an investigation be necessary, I will provide any necessary support to the best of my ability.

31. I confirm that should I become aware of any vulnerabilities to the CJSM I will raise it to the MoJ immediately.
32. I will inform my employers, CJSM Organisation Administrator or CJSM Helpdesk prior to departure in order that my account may be deleted.

Declaration:

I am fully aware of my responsibilities in relation to the use of the Service and as set out in these Terms & Conditions.

Signature	Name (please print)	Date	Position

Organisation name:

Please hand your signed copies of these Terms and Conditions to your organisation's administrator of CJSM.

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

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

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

More information on the Nation Cyber Security Centre and be found on their Website: https://www.ncsc.gov.uk/about-us