

CPSS Procedure for Controls Over Data Access and Storage On behalf of Surrey and Sussex LPC's

Introduction

CPSS implements physical and local access controls across its networks, IT systems and services to provide authorised, granular, auditable and appropriate user access, and to ensure appropriate preservation of data confidentiality, integrity and availability. It is vital that authorised users who have access to CPSS systems and information are aware of and understand how their actions may affect security. Information and data can be transferred and exchanged in a variety of ways, directly and indirectly. These may include:

- spoken word
- post, or e-mail
- internet or intranet
- magnetic media (including but not limited to CDs, DVDs, Memory Sticks)
- electronic file transfers and document sharing
- web portals

Definitions

- Physical access control refers to the selective restriction of access to a location.
- Logical access control is defined as restricting virtual access to data and consists of identification, authentication and authorisation protocols.
- Confidentiality: systems and information will only be access by authorised users.
- Integrity: the accuracy and completeness of systems and information are safeguarded.
- Availability: systems and information are physically secure and are accessible to authorised users when required.
- Authorised users refer to the following groups who either as a part of a contract of employment or third-party contract, have access to or use CPSS systems and information:
 - Chief Executive
 - Full and part time staff
 - LPC members
 - TECRES, IT providers

Purpose

The purpose of this policy is to ensure that both logical and physical access to information and systems is controlled and procedures are in place to ensure the protection of information systems and data.

Scope

The scope of this policy includes all access to CPSS information, systems and physical access to areas and locations where information and data is located. This policy applies throughout the information lifecycle from acquisition/creation, utilisation, storage and disposal. The policy is concerned with all information systems, digital and non-digital and will cover all information within CPSS that is or may be:

- stored on computers including use of SharePoint/OneDrive
- transmitted across networks
- printed out or written on paper
- sent internally or externally (by whatever method)
- stored on removable and other electronic media

Data Access

CPSS will provide all authorised users with access to the information they require to carry out their responsibilities in as effective and efficient manner as possible.

- CPSS controls access to information based on business and security requirements. The CEO and CPSS Exec have a responsibility to keep information access requirements for specific roles up to date and regularly reviewed.
- For systems containing restricted and personal information and data; access is restricted to the CEO, Business Administrator and CPSS Exec HR Lead.
- The access rights take into account:
 - Data protection and privacy legislation and any potential contractor/LPC commitments regarding access to data or services.
 - The 'need-to-know' principle (i.e. access is granted at the minimum level necessary for the role).
 - 'Everything is forbidden unless expressly permitted'.
 - The appropriate level of access to systems and information will be determined on the prospective users required business need, job function and role. User access requests are subject to authorisation and review. When authorisation is granted, unique log on credentials and passwords will be provided.
 - Generic logons are not generally permitted.

Information must only be transferred to persons who are authorised to have access to it and there should be adequate security measures in place at the virtual or physical destination.

Storage

- Information in all formats should be stored throughout its existence in an environment suited to its format and security classification, to protect it from threats to its physical integrity through unnecessary wear and tear, physical harm, specific risks such as a fire, flooding or extreme environmental fluctuations and security from loss or unauthorised access.
- Information whether original or duplicate, should never be kept outside of corporate systems, such as on personal drives or other removable media, except where necessary for example a temporary off-line copy because of a business need to work off-site or off-line or for an authorised transfer. Information held in digital formats should be managed and stored in such a way as to ensure usability and accessibility throughout its lifetime. This may involve migration of information between environments and systems, conversion to updated software versions, or from obsolete to current formats.
- Protection from unauthorised access may require mechanisms such as password protection or encryption of digital files and data or sign-in request sheets for access to non-digital information.
- Where information is stored on a mobile device (PDA, laptop, USB drive), special care must be taken to ensure that the device is protected from theft, loss, or damage, particularly if it is transferred or used away from CPSS sites.
- Physical access to information should be appropriately restricted by securing it in rooms, cabinets, drawers or other storage areas and by ensuring that files and computer monitors are not left open and unsecured to general or casual view.
- Individuals are personally responsible for those documents in their care.

Systems and information de-registration

If a member of staff changes their role or their contract is terminated, their line manager should ensure that the user's access to the system/information has been reviewed or if necessary, removed as soon as possible.



Breaches of Policy

Breaches of this policy and /or security incidents should be immediately reported to the CEO as quickly as possible. If a member of staff is deemed to have contravened any of the information in the policies or procedures, potentially jeopardising the availability, confidentiality or integrity of the systems or information, their access rights should be reviewed immediately by the system owners. Failure to comply with this procedure could result in action in line with the CPSS Disciplinary Procedure.

Reviewed: 8th April 2025
Next Review Date: April 2027