Data Breach Reporting Procedure

V1.0 March 2026

What is a personal data breach?

A personal data breach means "a breach of security, leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data".

It includes breaches that are the result accidentals or caused deliberately. It also means that a breach is more than just about losing personal data, or a cyberattack.

Common examples that arise in organisations like ELCAP include:

- accidentally sending emails with personal data to the incorrect recipient
- unauthorized access to physical files, such as sensitive paper documents or files are left out in common areas or unlocked filing cabinets, , leaving papers in photocopies or printer, where they are discovered by other staff without authorisation to have access, or allowing unauthorized personnel or visitors to access confidential information.
- improper disposal of documents, such as employees throwing away documents containing personal or confidential data in regular trash bins instead of shredding, making it possible for someone to retrieve and misuse the information.
- computing devices containing personal data being lost or stolen
- unauthorised alteration of records or files containing personal data; and
- loss of availability of personal data.

In the event of a suspected or potential data breach, it is crucial to respond quickly and appropriately to mitigate risk of negative impact and comply with legal obligations. Here is what is expected if you discover a suspected or potential data breach at ELCAP:

Contain the Breach

Take immediate action, if possible, to minimise risks and consequences of any suspected or potential data breach. Adopt a common-sense approach.

- If an email with confidential personal data has accidentally been sent to the incorrect recipient, try to recall or cancel sending it.
- When not possible, send a follow-up message explaining the mistake and asking the unintended recipient to delete and not misuse the information.
- If you find confidential records where they should not be, promptly remove them and keep them secure until you have discussed the breach with SMT.
- Secure systems as best you can to try preventing further unauthorised access.

Report the Breach Internally

- Report the data breach to a member of ELCAPs Senior Management Team immediately.
- Provide as much relevant information as possible, so they can evaluate risk and decide on appropriate action
- You will be advised if there is any further action expected, which may include disabling compromised accounts, changing passwords, or taking affected systems offline.

If you are in any doubt as to whether you should report something, it is always best to do so. A personal data breach may be serious, or it may be minor, and it may involve fault or not, but we always need to know about them to make a decision.

We may not need to treat the breach incident itself as a disciplinary matter – but a failure to report could result in significant exposure for ELCAP, and for those affected, so a failure to report will be a serious disciplinary matter.