Reporting Incidents

Information related to reporting information and cyber security incidents

It is important that staff can recognise information and cyber security incidents and are able to report these.

Data Protection (GDPR) incidents must be reported using the Data Incident Breach Management Procedures to the Councils Data Protection Officer. See related pages below.

To report a security incident use the following form:

- https://forms.office.com/Pages/ResponsePage.aspx?id=[**LINK REDACTED**]

What is a security incident?

A security incident is any actual or potential misuse, exploitation or unauthorised access to the ERC computing and network infrastructure, any program or code designed to self-replicate and cause malicious damage or business system disruptions. Infrastructure includes Council information assets, computer platforms, networks, gateways and applications.

Security Incident Examples:

PC Tampering: where someone has attempted to gain unauthorised access to a PC/laptop/handheld computer or to tamper with the integrity of the hardware to gain access to information on the device or to ERC's corporate or education networks.

Unauthorised Access to Restricted ERC Information: an attempt has been made or actual unauthorised access has been gained to restricted ERC information resources on any ERC computing platform. For example, it appears that someone gained unauthorised access to sensitive (client and service user data, Human Resource, payroll information, financial transaction, etc.) files residing on an ERC computing platform.

Internet Abuse: activity on the Internet that is outside of that allowed in the ERC Information Security Policy regarding Internet Usage. For example, using ERC resources to interfere with other computing systems, represent themselves as another person or for personal gain.

PC Controlled Remotely: It is possible for software (botnets) to be loaded to a PC remotely, which allows the remote user full control of the target machine without the user being aware.

Business data tampered with: Examples could be missing files, files with incorrect change dates, unauthorised copies of the files found elsewhere on the network or on PC hard drives.

Trojans and Viruses: Users may install Trojans and viruses, which result in unusual activities on the system. Examples may be missing files, increased system activity, increased email activity etc.

Social Engineering: An attempt by an unknown 3rd party to manipulate users into performing actions or divulging confidential information.

Report Lost or Stolen ICT Equipment

Record details of every loss or theft of hardware, including peripherals, to ensure an information risk assessment can be undertaken

It is important that any loss or theft of hardware that has the ability to hold information assets is recorded. This allows the Council to ascertain whether any risk is evident in relation to information assets retained on the equipment, device or peripheral.

Before reporting to security via this process please ensure you have a logged a ticket within the ICT Service Desk to ensure any technical requirements are addressed.
Staff are responsible for reporting such incidents to the Information Security Officer for the following to be ascertained:

- potential risk to information assets
- whether the Information Governance & Data Protection Officer needs to be advised
- whether local operating procedures need to be reviewed
- whether staff involved require support with additional training and / or guidance

Reporting the incident via online form

Use the online form to report an incident: https://forms.office.com/Pages/ResponsePage.aspx?id=[**LINK REDACTED**]

Once completed the Information Security and Digital Risk Officer will automatically be notified.

Reporting via a Word Document

Please complete the form below to report lost or stolen devices and pass completed form to Cathie Fraser, Information Security and Digital Risk Officer at cathie.fraser@eastrenfrewshire.gov.uk