ICT security incident handling guide

To report an ICT security incident, contact the ICT service desk on 0115 977 2010.

Do not give specific information about the security incident to the ICT service desk. The necessary information will be gathered entirely by the ICT Security Team when they contact you.

What is an ICT security incident?

An ICT security incident occurs when there is an event which has caused or has the potential to cause damage to the council's:

- information
- ICT assets
- reputation
- personnel.

Incidents can be accidental incursions or deliberate attempts to break into systems. They can be benign or malicious in purpose or consequence. Regardless, each incident requires careful response at a level commensurate with its potential impact to the security of individuals and the organisation as a whole.

Where council information is concerned, an ICT security incident is any event or set of circumstances threatening the confidentiality, integrity or availability of the information:

- **confidentiality**: the information is restricted to those rightfully needing to access and process it as part of their jobs
- **integrity:** there is confidence in the quality and reliability of the information ie it is correct, up to date and complete as opposed to inaccurate, out of date, corrupted or missing
- **availability**: the information can be rightfully accessed when needed. Access is not prevented by interference from any person or system.

How would I identify an ICT security incident?

An incident or suspected incident can be identified in many ways:

Malicious incident

- a computer becomes infected by a virus or other malware, (for example spyware or adware)
- finding data that has been changed by an unauthorised person
- receiving and forwarding chain letters – Including virus warnings, scam warnings and other emails which encourage the recipient to forward onto others

- unknown people asking for information (known as social engineering) which could gain them access to council data (eg a password or details of a third party)
- unauthorised disclosure of sensitive or confidential information electronically, in paper form or verbally
- deliberate damage to council equipment or services eg computer vandalism.

Access violation

- disclosing your login id and password credential to unauthorised persons
- writing down your password and leaving it on display or somewhere easy to find
- accessing systems using someone else's authorisation credentials eg someone else's user id and password
- allowing unauthorised physical access to secure premises eg server room, restricted areas.

Inappropriate use

- accessing inappropriate material on the internet
- sending inappropriate emails
- use of unapproved or unlicensed software on council equipment.

Theft/loss incident

- theft or loss of data – written or electronically held
- theft or loss of council equipment, for example computers, monitors, mobile phones, memory sticks, CDs etc.

Accidental incident

- sending an email containing sensitive or confidential information to 'all staff' by mistake
- receiving unsolicited mail of an offensive nature, eg containing pornographic, obscene, racist, sexist, grossly offensive or violent material
- receiving unsolicited mail which requires you to enter personal data.

The above list is not exhaustive.

Your Responsibilities

The security of council data is the responsibility of every individual working for the council. All users need to protect data at all times.

Everybody has a role to play and a contribution to make to the safe and secure use of ICT equipment and the information that it holds.

You **must not** use council ICT equipment or services in a way that could:

- bring the council into disrepute

- cause offence
- interfere with council work
- jeopardise the security of data, networks, equipment or software.

You must report all security incidents that come to your attention to both:

- your line manager (or their nominee)
- the ICT Security Team (through the ICT service desk).

Role of the ICT Security team

If you report an ICT security incident, the ICT Security team will contact you to gather further information. This information includes:

- date and time the incident occurred
- location of the incident
- the type of data or information involved
- location of data or equipment(s) affected
- whether the loss of any data put any person(s) or other data at risk
- number of users reporting the incident.

The above list is not exhaustive.

ICT security incidents reported to the ICT Security team will always be handled confidentially and investigations will be conducted according to council policies.

Depending on the nature of the incident reported, an investigation could go in two directions:

- ICT finds a way to avoid a repetition of the incident
- evidence is uncovered which leads to action being taken against a user under the council's rules, regulations and security policies.

Privacy

Your right to privacy will always be respected.

Intrusive examinations of your activity, such as email or internet usage, will only be performed if absolutely necessary and justified in the circumstances. Where this is necessary management authorisation will be obtained before proceeding with an investigation.

Further information

If you would like further information on ICT security incidents, or on any matters relating to ICT security, please contact the ICT service desk