Information security incidents

Information Security Processes

Information security incidents

The Council has created a new e-form for you to notify us about an information security incident. We need to ensure that the security of information is maintained at all times. The council acknowledges that sometimes things can go wrong and if it does, needs to know about this so that it can take action to recover information, mitigate against the impact on individuals, and ensure that the issue does not happen again.

We have a process for dealing with information security incidents which is set out below.

What we mean by information security incidents

As a Council, we collect certain types of information about the citizens of Kirklees, in order to provide them with a service. This might include names, addresses, dates of birth, and more sensitive information such as ethnicity, and health and social care records. We have a legal obligation to ensure that this personal information is kept securely. Where there is any kind of loss of this information, this is known as an information security incident, and could lead to a data breach.

Information security incidents come in many shapes and sizes. They include, but are not limited to:

- The loss or theft of data or information;
- Sending information in an email or item of post to the wrong person;
- Attempting (successfully or not) to gain unauthorised access to personal information in a computer system or hard copy documents;
- Accessing computer systems or hard copy documents without a legitimate business need to access it or approval from a senior manager;
- Unauthorised disclosure of personal or confidential information to a third party, including discussing personal information in a public place where you can be overheard.

More examples of some of the more common forms of Information Security Incidents are at the end of this page.

Real examples

People often think of a data breach being related to breaches of cyber security, and therefore an IT issue. Of course, IT is an important issue, and there are some useful IT security top tips provided by the Information Commissioner's Office (ICO). But in fact, the highest number of information security incidents reported to the ICO involve the following:

- Data posted to the incorrect recipient;
- Loss or theft of paperwork;
- Data sent by email to the incorrect recipient.

You can see further details about the number and type of breaches reported to the ICO here.

Why you need to know

As you can see from the above, information security is not just an IT issue, but an issue for everyone. We all have a duty to make sure that we are keeping individuals' personal information safe. The possible consequences for the individual or individuals concerned, and for the Council, can be enormous.

The quicker a potential information security incident is discovered, reported, and investigated, the quicker we can contain the incident and mitigate the risks involved.

The possible consequences

- Loss of an individual's personal data can be distressing and damaging for them, and can even put the individual at risk. They could face discrimination, damage to their reputation, financial loss, loss of confidentiality or other significant economic or social disadvantage.

- Loss of someone's personal data can cause terrible reputational damage to the organisation as a whole. You may remember the news coverage around the TalkTalk data breach.

- Information security incidents can mean that action is taken against us by the Information Commissioner's Office. This can include huge fines of up to £500,000. These are set to rise under new legislation (GDPR) in May 2018 to a whopping 20 million euros (currently £18,400,000). Just as an example, a data breach by Devon County Council resulted in a fine of £90,000. Our best guess is that when GDPR comes in, a similar breach could incur a fine of between £3.6 and £7 million.

- If an incident isn't reported, it could make matters much worse should it be discovered at a later date – including significantly increasing the chance of a huge fine.

What do I need to do when things go wrong?

Report it quickly!

Information Security Incidents need to be reported as soon as possible so they can be assessed by the Information Governance team to help identify any risks to the people whose information has been compromised and / or the Council's systems. It is vital to gain as much information as possible from the colleagues to identify what has happened. As soon as information systems or data are suspected to be, or are actually affected by an adverse event which is likely to lead to a security incident, you need to alert a manager to this and report this to the Information Governance Team by using the online reporting form

If you need to contact the Information Governance Team, please do so via Lync (01484 221000 and ask for Data Protection). Or email infosec@kirklees.gov.uk

Once received by the Information Governance Team, the incident will be assessed to determine whether it meets the threshold for notifying to the Information Commissioner's Office (ICO), the independent regulator for information rights in UK.

The Information Governance Team will liaise with the reporting officer and / or appropriate managers to gain further information if required before making a decision about notification to the ICO.

Managers within the Service(s) in which incident arise are expected to investigate and manage the incident to recover or contain the information, mitigate against any negative impact for the individuals whose data has been compromised and take action accordingly. The Information Governance Team, HR, IT and others as appropriate can assist managers with this.

Once a decision on notification to the ICO has been made, the Service will be notified of this.

Action you need to take now

- Think about the personal data you deal with within you team. Treat it with respect – as though it was your own! – and keep it safe.

- Make sure you have completed the mandatory data protection e-learning available on MiPpod Xtra. This was updated in 2017.

- Think about whether you have had any near misses within your own team recently. By a near miss, we mean something small that went wrong, **without** any loss of personal data. This could be a letter that went to the wrong address but was returned unopened. Or an email that went to the wrong person – but that person was a Council employee, who informed you and immediately deleted the email. These near misses don't need to be reported to the IG team, but you should let your manager know so they can help the team to address any issues and prevent it from happening again, or from escalating to a data breach. Near misses tell you that you need to look at your processes, your record keeping, and/or the level of training within your team to see where improvements can be made.

- Follow guidance that's readily available to help you, such as the Clear Desk Clear Screen Guide; the guidance on sending sensitive information using email; and our previous Spotlight message on using email.

Key Messages

- Keep information security foremost in your mind when using personal data (either verbal, electronic or paper) to prevent an incident occurring.
- All staff should report any incidents or suspected incidents immediately to their own senior management, and the Information Governance team via the online reporting form
- If you are unsure of anything in this document you should ask for advice from the Information Access Team (01484 221000 and ask for Data Protection, or email infosec@kirklees.gov.uk)

Learning from information security incidents

The Council recognises that there are risks associated with people accessing and handling information in order to conduct official council business.
The process of managing Information Security Incidents aims to mitigate the following risks:

- To reduce the impact of actual or potential breaches by ensuring incidents are followed up correctly.
- To help identify areas for improvement to reduce the risk and impact of future incidents.

Non-compliance with this process and the content of this document could have a significant effect on the efficient operation of the Council and may result in risks to the individual(s) whose personal information is compromised, financial loss to the Council, an inability to provide necessary services to our customers and disciplinary proceedings or prosecution of individuals.

To learn from incidents and improve the response process, incidents must be recorded; the Information Governance team will review:

- Types of incidents reported
- Volumes of incidents

The information will be collated and reviewed on a regular basis by the Information Governance team and any patterns or trends identified. Any changes to the process made as a result will be noted and implemented.

The information, where appropriate, will be shared with the Information Governance Board. The Information Governance team will advise Services accordingly on learning / improvements they may wish to make to their practices and procedures.

Information Security Incident Examples

Examples of the most common Information Security Incidents are listed below. It should be noted that this list is not exhaustive.

Contract Issue	Insecure disposal of personal information in contravention of requirements of a contract Lack of a written contract with a data processor which contains the appropriate data protection clauses
IT Issue	Deletion of electronic drives or documents Clicking a link in a malicious email
Loss: Email (external)	Email containing personal information or sensitive council information sent to wrong recipient external to the council Email sent to group of external recipients with email addresses in To or CC field
Loss: Email (internal)	Email containing personal information or sensitive council information sent to wrong recipient internal to the council Email containing personal information or sensitive council information, including where identity of recipients is sensitive, sent to group of internal recipients with email addresses in To or CC field
Loss: Mail	Item of mail containing personal information or sensitive council information sent to wrong address Item of mail sent to correct address but containing personal information re a third party
Staff Action: Access to System	Access to personal information held within a Council system which is not for a business purpose, ie the member of staff accessing the information is not actively involved in providing a service or supporting officers who are providing a service. For example, looking at information relating to a family member, friend, neighbour, colleague, etc, out of interest.
Staff Action: Disclosure	Giving information to someone who should not have access to it - verbally, in writing or electronically
Staff Action: Insecure Storage	Leaving personal information or sensitive council information on a desk or in an unlocked cupboard where is can be accessed by others people (officers or members of the public)
Staff Action: Insecure Transfer	Emailing personal information or sensitive council information through normal council email addresses to external email addresses; ie not using a council GCSX account, or using a council GCSX account but sending it to a non-secure email address
Staff Action: Loss	Leaving a bag of papers containing personal information or sensitive council information on public transport (even if it has subsequently be retrieved) Leaving council ICT equipment in a public place Losing papers or equipment containing personal information or sensitive council information
Theft: Council Building	Theft of papers or equipment containing personal information or sensitive council information from a council building following a burglary or unauthorised access to council building
Theft: Officer Home/Car	Theft of papers or equipment containing personal information or sensitive council information from an officer's home or vehicle