Norfolk County Council

Data Breaches and IT Security Breaches - Report and Contain Procedure

If you are reading a printed version of this document you should check the Information Management pages on iNet to ensure that you have the most up-to-date version.

Personal Data Breach is defined under Article 4(12) of the General Data Protection Regulations (GDPR) as:

"a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed."

These procedures apply to all personal data breaches including (as a rule of thumb) (a) data breaches by individuals and (b) IT security breaches:

These can be:

(a) Data Breaches by individuals
Examples
• Loss or theft of paper records or loss or theft of equipment on which data is stored e.g. laptop, mobile phone, tablet device, memory stick
• Letter or email containing personal and/or confidential data sent to the wrong address (including County Council staff or third parties) or an email to unauthorised group email boxes
• Personal data disclosed orally in error in a meeting or over the phone to County Council staff or to third parties – including "blagging" where information is obtained by deceiving the County Council, or where information has been disclosed without confirming the true identity of the requester
• Unauthorised access to County Council information classified as personal or confidential e.g. attaching documents to an outlook diary appointment that is openly accessible
• Posting information on the internet or on a computer otherwise accessible from the internet without proper information security precautions

• Sensitive information left on the photo-copier, on a desk, or in a meeting room in County Council premises
• Unauthorised alteration or deletion of County Council information
• Not storing personal and confidential information securely
• Not ensuring the proper transfer or destruction of files after closure of offices/buildings eg not following building decommissioning procedures
• Failure to safeguard/remove personal data on office equipment (including computers and smart phones) before disposal/sale
• Loss of mobile devices (e.g. laptops, mobiles phones, memory sticks; hard drives)
• Divulging a password to another user without authority
(b) IT Security Breaches
Examples
• Unauthorised access to the IT systems because of misconfigured and/or inappropriate access controls
• Hacking or phishing attack and related suspicious activity
• Virus or malware attacks and related suspicious activity
• IMT infrastructure-generated suspicious activity

Who does this apply to?

This procedure applies to members, staff and managers

	What must I do?	Why?	How?
	DATA BREACHES		
1	**MUST:** If you discover a **data breach**, you must **immediately** report the matter to your line manager and to the Information Compliance Team	• Article 33 of the GDPR places a duty on the Council to report a data breach to the Information Commissioner's Office (ICO) not later than 72 hours after becoming aware of it if the breach is likely to result in "a risk to the rights and freedoms of others" • Article 34 of the GDPR places a duty on the Council to inform the data subject without undue delay if the breach is likely to result in "a high risk to the rights and freedoms" of the data subject • Failure to comply with these requirements will be a breach of the GDPR which may result in a substantial fine for the Council. • In order to be able to assess the severity of the risk, investigate and report to the ICO within the timescale and to notify the data subject if necessary, the breach must be reported **immediately**	• Inform your line manager • Inform the Information Compliance Team – see paragraph 3 below

2	**MUST**: The line manager must **immediately** seek to contain the breach if necessary and recover any information disclosed as a result of the breach If the manager has any difficulties in containing the breach (e.g. because of the scale of the breach) they **must immediately** discuss the matter with the Information Compliance Team Manager or, in their absence, another manager in the Information Compliance Team	To ensure that any damage caused by the breach is contained (for example, by ensuring that any emails sent to the wrong person have been deleted) and to ensure that the matter is properly assessed and investigated if necessary	• Establish who needs to be made aware of the breach and tell them what they are expected to do to help contain it. This could be: ▪ isolating or closing a compromised section of the network, ▪ finding a lost piece of equipment ▪ changing the access codes at the front door ▪ ask recipients to delete unread emails that have been sent to them in error. • Establish if there is anything that can be done to recover any losses and limit the damage the breach can cause. As well as the physical recovery of equipment, this could involve ▪ the use of back up tapes to restore lost or damaged data or ▪ ensuring that staff recognise when someone tries to use stolen data to access accounts ▪ Collect letters that have been sent to the wrong address.

3	**MUST**: The line manager must also **immediately** report any breach to the Information Compliance Team Manager or, in their absence, another manager in the Information Compliance Team as soon as possible after receiving the report of the breach	• The GDPR (Article 33) places a duty on the Council to report a data breach to the Information Commissioner's Office (ICO) not later than 72 hours after becoming aware of it if the breach is likely to result in "a risk to the rights and freedoms of others" • In order to be able to assess the severity of the risk, investigate and report to the ICO within the timescale, the breach must be reported **immediately**	• By phone to the Information Compliance Team duty line • By completing the Data Breaches and Security Incidents Report Form in as much detail as possible and sending to the Information Compliance Team Manager marked "urgent" at information.management@norfolk.gov.uk
4	**MUST:** If you discover an **IT security breach**, or a data breach involving the loss or theft of IT equipment, you must **immediately** report the matter to your line manager **and** to the ICT Service Desk	• The GDPR (Article 33) places a duty on the Council to report a data breach to the Information Commissioner's Office (ICO) not later than 72 hours after becoming aware of it if the breach is likely to result in "a risk to the rights and freedoms of others • In order to be able to assess the severity of the risk, investigate and report to the ICO within the timescale, the breach must be reported **immediately**	• Inform your line manager • Inform the ICT Service Desk by contacting the Service Desk on 01603 495800 • Inform the Information Compliance Team – see paragraph 6 below

5	**MUST**: The ICT Service Desk and, if necessary, the line manager must **immediately** seek to contain the incident and, if necessary, recover of any information disclosed as a result of the incident If there are any difficulties in containing the breach (e.g. because of the scale of the breach) the ICT Service Desk or Team Manager **must immediately** discuss the matter with the Information Compliance Team Manager or, in their absence, another manager in the Information Compliance Team	To ensure that any damage caused by the breach is contained and to ensure that the matter is properly assessed and investigated if necessary	• ICT Service Desk will agree with the Team Manager how incident should be contained • ICT will follow its internal Security Incident Management Process to ensure that incident is contained
6	**MUST**: The line manager must **immediately** report the security incident to the Information Compliance Team Manager as soon as possible after receiving the report of the breach	• The GDPR (Article 33) places a duty on the Council to report a data breach to the Information Commissioner's Office (ICO) not later than 72 hours after becoming aware of it if the breach is likely to result in "a risk to the rights and freedoms of others" • In order to be able to assess the severity of the risk, investigate and report to the ICO within the timescale, the breach must be reported **immediately**	• By phone to the Information Compliance Team duty line • By completing the Data Breaches and Security Incidents Report Form in as much detail as possible and sending to the Information Compliance Team Manager marked "urgent" at information.management@norfolk.gov.uk

	DATA BREACHES AND IT SECURITY INCIDENTS		
7	**MUST**: Within 24 hours of receipt of the report form the Information Compliance Team Manager must carry out a risk assessment of the breach/security incident to: (a) Carry out a preliminary assessment regarding the need to notify the ICO and inform the data subject (b) Assess whether the risk in relation to the breach/security incident is serious, high, medium or low and to confirm the type of investigation/action to be carried out, ie • Level 1: Investigations into [serious/high risk breaches/security incidents] • Level 2: Investigations into [medium/low risk breaches/security incidents] where we think that an investigation will assist us in learning from mistakes • Level 3: Fast track investigation into [medium/low risk breaches/security incidents] where we think that a Level 2 investigation is unnecessary to assist us in learning from mistakes	To: • Understand how breaches/security incidents occur • Learn lessons • Improve systems and services • Arrange for breaches likely to result in "a risk to the rights and freedoms of others" to be reported to the ICO • Arrange for the data subject to be notified if likely to result in a high risk to the rights and freedoms of the data subject	Apply the Data Breaches and IT Security Breaches Investigation Process

What if I need to do something against the procedure?

If you believe you have a valid business reason for an exception to this procedure, contact your manager or business lead for advice.

If your manager/business lead concludes that there should be an exception, the Information Management Team **must** be informed in writing with reasons within 24 hours of the proposal.

If there is any uncertainty about the issue contact the Information Management Team for advice.

References

Data Breaches and IT Security Breaches Investigation Process

Data Breaches and Security Incidents Report Form

Security Incident Management Process *(ICT internal process)*

General Data Protection Regulations

Article 29 Working Party Guidelines on Personal Data Breach Notification under Regulation 2016/679

Data Protection Act 2018

Common law duty of confidentiality

Human Rights Act 2000

Breach Statement

Breaches of information policies will be investigated and may result in disciplinary action. Serious breaches of procedure may be considered gross misconduct and result in dismissal without notice, or legal action being taken against you.