Information Security Incident Management

The Information Security Breach Management Policy seeks to outline the measures to be taken by the Council when dealing with a personal data breach. It applies to information in all forms, whether manual or computerised. The aim of this policy is to ensure that the Council reacts appropriately to any actual or suspected security incidents relating to information systems and data. Appropriate action following a breach is required to ensure containment and recovery, business continuity and to avoid further breaches of the law and statutory, regulatory or contractual obligations.

Personal Data Breaches

A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are caused accidentally or deliberately.

A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data. There will be a personal data breach whenever any personal data is:

- lost,
- destroyed,
- corrupted,
- disclosed to someone who shouldn't have access to it, or
- made unavailable, for example, when it has been encrypted by ransomware, or a power outage.

A personal data breach can happen for a number of reasons, including:

- Loss or theft of data or equipment on which data is stored including paper files;
- Inappropriate access controls allowing unauthorised use;
- Equipment failure;
- Coding error in an IT system;
- Human error;
- Inappropriate disposal of information;
- Unforeseen circumstances such as a fire or flood;
- Power cut;
- Hacking, virus or ransomware attack;
- 'Blagging' offences where information is obtained by deceiving the organisation who holds it. (This is also referred to as "social engineering");
- The transfer of data or information to those who are not entitled to receive that information;
- Successful attempt to gain unauthorised access to data or information storage or a computer system; and
- The unauthorised use of an authorised system.

Any breach, however it occurs, can have far reaching consequences. It could cause potential harm and distress to individuals or seriously compromise the integrity and

security of the Council's IT systems. As a result, this Policy seeks to recognise the following four important elements:

- Containment and recovery;
- Assessment of ongoing risk;
- Notification of breach; and
- Evaluation and response.

Some security incidents will not amount to a personal data breach because they do not affect the confidentiality, integrity or availability of personal data. Such security incidents will be regarded as 'near misses' and, recognising that they could result in a future personal data breach, appropriate action will taken by the relevant Service Manager to ensure that they do not occur again and reported to the Data Protection Officer. Example of security incidents include:

- Use of unapproved or unlicensed software on the Council's equipment;
- Use of unapproved or unauthorised hardware on the Council's network/equipment;
- Sharing user id and password with someone else;
- Writing down a password and leaving it on display / somewhere easy to find;
- Responding to or following links in unsolicited mail which require entry of personal data;
- Failed attempts to gain unauthorised access to data or information storage or a computer system;
- Allowing access to secure parts of the council's buildings to unauthorised individuals.

This Policy sets out the Council's approach to dealing with Personal Data breaches.

Responsibilities

Overview

The Council is under an obligation to notify the Information Commissioner of certain personal data breaches without undue delay, but not later than 72 hours after becoming aware of it. As time is of the essence, it is imperative the Data Protection Officer is notified straightaway and any investigation prioritised.

All staff shall ensure that:

- All breaches of information security, the General Data Protection Regulation (GDPR) and the Data Protection Act (DPA), actual or suspected, are reported to a line manager or Service Manager immediately. Where the line manager or Service Manager is not available immediately the breach must be reported to the Data Protection Officer immediately;
- All breaches of information security, the GDPR and the DPA, actual or suspected, which occur or are discovered outside of normal office hours are reported to the Data Protection Officer immediately and not left until the

following working day as soon as the Council offices are open to ensure that the report has been received and it being dealt with;
- They co-operate fully with any investigation following a breach and provide all necessary information; and
- They report any instances where this Policy has been or is being violated to the ICT Helpdesk, ext 3888.

All Line Managers and Service Managers shall ensure that:

- All breaches of information security, the GDPR and the Data Protection Act, actual or suspected, are reported to the Data Protection Officer immediately;
- They co-operate fully with any investigation following a breach and provide all necessary information to the Data Protection Officer; and
- They take the lead on investigating the breach and ensure the investigation is completed as a priority.

The Data Protection Officer or deputy will:

- Determine whether a breach should be reported to the Information Commissioner (ICO);
- Report notifiable breaches to the ICO and liaise with the ICO during the course of any investigation;
- Establish who needs to be made aware of the breach and inform them what they are expected to do to assist in the containment exercise. This could be isolating or closing a compromised section of the network, finding a lost piece of equipment or simply changing the access codes at the front door;
- Establish whether there is anything the Council can do 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;
- Assess the risks associated with the breach, which requires consideration of how serious or substantial they are and how likely they are to happen. This includes risks to the Council's IT systems and potential adverse consequences for individuals;
- Consider what steps need to be taken to prevent further breaches;
- Consider what other agencies may need to be informed depending on the type and severity of the breach;
- Consider whether Warning, Advice and Reporting Point (EMG Warp) should be consulted.

The Data Protection Officer may require assistance from the members of the Data Security Group who shall provide such support as is necessary as a matter of priority.

The Service Manager shall:

- Consider the information gathered as part of the investigation and implement the steps which need to be taken to:

- contain the breach and recover any losses; and
- reduce or remove any ongoing risks; and
- prevent any further breaches.

Notification of Breaches

Notifying the Information Commissioner

There is a legal obligation on the Council, as a data controller, to report personal data breaches to the Information Commissioner unless the breach is unlikely to result in a risk of significant adverse effects on individuals, such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the person concerned.

Whether to notify the ICO will be determined on a case by case basis, but the following will be considered when making the decision:

- the potential adverse consequences for the affected individuals,
- how serious or substantial those adverse consequences are, and
- how likely they are to happen.

Relevant guidance will also be taken into account.

Failing to notify a breach to the ICO when required to do so could result in a significant fine up to 10 million euros.

The Data Protection Officer or deputy will decide whether to notify the ICO.

Notifying Individuals

The Council recognises that not every incident will warrant notification and notifying everyone whose details are held on a database of an issue affecting only a small proportion of those people may well cause disproportionate enquiries and work.

If a breach is likely to result in a high risk to the rights and freedoms of individuals, the Council must inform those concerned directly and without undue delay.

A ‘high risk’ means the threshold for informing individuals is higher than for notifying the ICO. The Council will assess both the severity of the potential or actual impact on individuals as a result of a breach and the likelihood of this occurring. If the impact of the breach is more severe, the risk is higher; if the likelihood of the consequences is greater, then again the risk is higher. In such cases, the Council will need to promptly inform those affected, particularly if there is a need to mitigate an immediate risk of damage to them. One of the main reasons for informing individuals is to help them take steps to protect themselves from the effects of a breach.

Individuals affected will be notified if necessary to enable them to take steps to protect themselves, for example by cancelling a credit card or changing a password, or to allow the appropriate regulatory bodies to perform their functions, provide advice and deal with complaints. When notifying individuals, the Council will endeavour to give them specific and clear advice on the steps they can take to protect themselves and also what the Council is able to do to help them.

The Data Protection Officer or deputy in consultation with the Monitoring Officer will decide whether to notify affected individuals.

Notifying the Press

When considering whether to inform the media, the Council will balance the need to be open and transparent with the need to protect the interests of those individuals who may suffer distress at having the breach reported in the press, together with the risks of unscrupulous individuals who may seek to take advantage of the situation. Advice will be sought from the Council's Communications Team prior to any decision being made as to what, if anything is reported.

The Chief Executive will determine whether it is appropriate to notify the press.

Notifying CESG GovCertUK

GovCertUK is responsible for providing support to local authorities when responding to computer security incidents. As a member of Public Services Network, the Council is required to report critical and significant security incidents to GovCertUK.

The CESG categorises incidents (depending on their scope, number of users affected, ability of the Council to deal with the situation and impact), into Negligible, Minor, Significant and Critical categories. Some examples are:

Negligible: Spam, Quarantined viruses, network monitoring alerts on single PCs.
Minor: Unsuccessful denial of service on a single PC, single PC unauthorised access.
Significant: Successful denial of service on a server, website defacement.
Critical: Targeted attack on our network infrastructure, unauthorised access to a server.

Generally Significant and Critical incidents have to be reported, minor can be reported for information collation purposes while negligible incidents do not have to be reported. The document also discusses which agencies should be informed about different types of incidents.

The Director responsible for ICT will decide whether to notify CESG GovCertUK. In doing so, they will take into account the CESG GovCertUK Incident Response Guidelines which apply at that time.

Public Services Network (PSN) / CINRAS

For incidents that impact on Public Services Network, the "Incident and Problem Management" process manual should be consulted and if appropriate the incident reported to the PSN Security Manager.

CINRAS shall be notified for incidents involving HMG approved cryptographic equipment.

The Director responsible for ICT will decide whether to notify the PSN Security Manager.

Notifying other agencies/organisations

The Council will consider notifying third parties such as the police, insurers, professional bodies, bank or credit card companies who can assist in reducing the risk of financial loss to individuals, and trade unions.

The Data Protection Officer or deputy in consultation with the Monitoring Officer will decide whether to notify other agencies.

Emergency Situations

The Council recognises that that there may be instances where immediate action is necessary to contain a breach and prevent further incident. An example is where there is a targeted attack resulting in a serious breach of network security. This would require immediate action to shut down the Council's network. It would not be practical or reasonable for a full investigation to be carried out prior to taking action. Instead, the Customer Services & IT Manager and IT Technical Manager have the authority to take whatever action they deem necessary in the circumstances and would follow the procedure outlined above to determine what further action should be taken. The incident will however be reported to the Data Protection Officer as outlined above.