SECURITY INCIDENT AND DATA BREACH POLICY

1. Scope

1.1 The scope of this Policy applies to all Northumberland IFCA employees and Members. Agency workers or sub-contractors who are required to use Northumberland IFCA's information systems will also be made aware of and be expected to abide by this policy. This is also relevant to organisations processing Authority data.

2. Purpose

2.1 To have a standardised management approach throughout the Authority in the event of a serious security incident or data breach by having clear policies and procedures in place. Fostering a culture of proactive reporting and logging will help reduce the number of incidents and breaches which often go unreported and unnoticed – sometimes, over a long period of time and often without resolution.

2.2 Incident management is the process of handling incidents and breaches in a controlled way ensuring they are dealt with efficiently, with a consistent approach to ensure that any damage is kept to a minimum and the likelihood of recurrence is reduced by measures taken.

3. Introduction

3.1 Northumberland IFCA is responsible for the processing, security and integrity of all information it holds. The Authority must protect this information using all means necessary by ensuring at all times that any incident which could cause damage to the Authority's assets and reputation is prevented and/or minimised as well as damage or distress to the data subject.

3.2 An incident or breach is defined as any event, any suspicion that an event has occurred, or any discovery or suspicion that vulnerability has been exploited to pose a threat to the confidentiality, integrity, or availability of information assets.

3.3 Classes of threat are listed below.

3.3.1 Threats to confidentiality

- These events may include attempts to gain access to an information asset for the purposes of obtaining information that the individual would not be authorised to have. The reverse may also occur if restricted information were placed in a publicly accessible location, either inadvertently or purposely, thus constituting a threat to confidentiality and a possible violation of the law.

  Incident classes: Disclosure, Unauthorised access, Password sharing.

3.3.2 Threats to integrity

- These are errors, intentional acts, and natural or accidental events that can result in the corruption or loss of information stored in, processed on, or transmitted by the Authority and its data processors. Corruption may be caused by fraud or associated with a disruption of service resulting from unauthorised modification, system failure or procedural error, even though the intent of such incidents may not have been deliberate. Misuse is a growing concern because it covers email, Internet, image files or even individuals doing private work.

Incident classes: Fraud, Unauthorised modification, Power failure, Procedural errors and Misuse.

3.3.3 Threats to availability

- These are events that may be caused deliberately or accidentally by individuals who cause disruptions in processing or loss of stored or transmitted information. Examples include wilful damage, power failure, procedural errors or theft. Malicious software is now taking many forms including denial-of-service attacks utilising some operating system or network exploit, viruses, worms, spoofing and email spamming.

  Incident classes: Theft; Malicious Software; Wilful damage; System failure.

4. Types of security incident

4.1 An incident is classified as serious when the incident:

- Involved actual or potential failure to meet the legislation to protect information such as the GDPR;
- Potentially involves or could lead to a data breach.

4.2 Some examples of serious incidents are:

- Loss or theft of IT equipment or information;
- Disclosing personal information to someone not authorised to have it;
- Unauthorised access to information;
- Breach of physical building security;
- Uploading personal information to a website in error;
- Human error resulting for example in personal information being left in an insecure location;
- Hacking into IT systems;
- 'Blagging' offences where information is obtained by deception.

5. Reporting Security Incidents (Including potential or actual data breaches) - Identification and Classification of security incidents

5.1. Security incidents (including a data breaches) must be reported to the Information Governance Team as soon as it has been identified in accordance with the Authority's Security Incidents and Data Breach Procedure.

5.2 Details of security incidents can be very sensitive and any sensitive information must be handled with discretion and only disclosed to those who need to know the details.

5.8 The Information Governance Team will determine whether it is a security incident or data breach and will allocate it in accordance with the appropriate management plan. Employees must not attempt to conduct their own investigations, unless authorised to do so, to ensure evidence is not destroyed.

5.9 The Authority's Senior Information Risk Owner (SIRO) and the relevant director are ultimately responsible for making any decisions.

5.11 The data breach or security incident will be concluded when the investigation is complete.

6. Training and Awareness

6.1 All staff and Members need to be introduced to their basic responsibilities under the GDPR in regard to protecting the data we hold and the systems that we use, which includes understanding what is an incident and how to report it. To ensure that they are aware, they will need to complete a mandatory training module in Information Security and Data Protection in addition to reading this policy.

6.2 Some members of staff employees will require further training and guidance. Those employees will be identified through their work and initial discussion with their line manager.

7. Compliance

7.1 Any violation of this policy and supporting procedure will be investigated and if the cause if found to be willful disregard or negligence, it may be treated as a disciplinary offence. All disciplinary proceedings are coordinated through the Human Resource Department.

8. Implementation

8.1 This policy is effective immediately.

9. Monitoring and review

9.1 This procedure will be monitored by the CEO and will be reviewed every two years or where there are changes to legislation.

10. Useful contacts

The Information Commissioner's Office via www.ico.org.uk

DATA BREACH PROCEDURE

Procedure Statement

Northumberland Inshore Fisheries and Conservation Authority (NIFCA) holds a substantial amount of personal and sensitive data. Every care is taken to protect personal data and to avoid a data protection breach. In the unlikely event of data being lost or shared inappropriately, it is vital that appropriate action is taken to minimise any associated risk as soon as possible. This breach procedure applies to all personal and sensitive data held by NIFCA. This procedure applies to all Authority Officers including Members, referred to herein after as ‘Officers’.

Purpose

This breach procedure sets out the course of action to be followed by all Officers at NIFCA if a data protection breach takes place.

Legal Context

The GDPR makes provision for the regulation of the processing (use) of information relating to individuals, including the obtaining, holding, use or disclosure of such information.

Types of Breach

Data protection breaches could be caused by a number of factors. Some examples are:

- Loss or theft of Officer or member data and/ or equipment on which data is stored;
- Inappropriate access controls allowing unauthorised use;
- Equipment Failure;
- Human Error;
- Unforeseen circumstances such as fire or flood;
- Hacking;
- ‘Blagging’ offences where information is obtained by deception.

Immediate Containment/Recovery

In discovery of a data protection breach, the following steps should be followed:

1. The person who discovers/receives a report of a breach must inform the DPO or, in their absence, either the CIFCO or the CEO. The DPO will inform the CEO of the breach. If the breach occurs or is discovered outside normal working hours, this should begin as soon as is practicable.

2. The DPO (or nominated representative) must ascertain (with the support of the CEO and other relevant Officers) whether the breach is still occurring. If so, steps must be taken immediately to minimise the effect of the breach. An example might be to shut down a system, or to alert relevant persons such as the IT support/ web-hosters.

3. The DPO/CEO (or nominated representative) must inform the Chair of the Committee as soon as possible. It is the Authority’s responsibility to take the appropriate action and

conduct any investigation.

4. The DPO/CEO (or nominated representative) must also consider whether the Police need to be informed. This would be appropriate where illegal activity is known or is believed to have occurred, or where there is a risk that illegal activity might occur in the future.

5. The DPO/CEO (or nominated representative) must quickly take appropriate steps to recover any losses and limit the damage. Steps might include:

   a. Attempting to recover lost equipment.

   b. Contacting the Authority Officers (with @nifca.gov.uk email addresses), so that they are prepared for any potentially inappropriate enquiries ('phishing') for further information on the individual or individuals concerned. Consideration should be given to a global email to all Authority Members and partner agencies. If an inappropriate enquiry is received by Officers, they should attempt to obtain the enquirer's name and contact details if possible and confirm that they will ring the individual making the enquiry back.

      Whatever the outcome of the call, it should be reported immediately to the DPO/CEO (or nominated representative).

   c. The use of back-ups to restore lost/damaged/stolen data.

   d. If bank details have been lost/stolen, consider contacting banks directly for advice on preventing fraudulent use.

   e. If the data breach includes any entry codes or IT system passwords, then these must be changed immediately and the relevant agencies and members of Officers informed.

6. Consider if this breach needs to be reported to the ICO. If so, it MUST be done so within 72 hours of the data breach. To identify if this is required, consider the following:

> When a personal data breach has occurred, you need to establish the likelihood and severity of the resulting risk to people's rights and freedoms. If it's likely that there will be a risk then you must notify the ICO; if it's unlikely then you don't have to report it. However, if you decide you don't need to report the breach, you need to be able to justify this decision, so you should document it.
>
> In assessing risk to rights and freedoms, it's important to focus on the potential negative consequences for individuals. Recital 85 of the GDPR explains that:
>
> *"A personal data breach may, if not addressed in an appropriate and timely manner, result in physical, material or non-material damage to natural persons 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 natural person concerned."*
>
> This means that a breach can have a range of adverse effects on individuals, which include emotional distress, and physical and material damage. Some personal data

breaches will not lead to risks beyond possible inconvenience to those who need the data to do their job. Other breaches can significantly affect individuals whose personal data has been compromised. You need to assess this case by case, looking at all relevant factors.

Investigation

In most cases, the next stage would be for the DPO/CEO (or nominated representative) to fully investigate the breach. The DPO/CEO (or nominated representative) should ascertain whose data was involved in the breach, the potential effect on the data subject and what further steps need to be taken to remedy the situation. The investigation should consider:

- The type of data;
- Its sensitivity;
- What protections are in place (e.g. encryption);
- What has happened to the data;
- Whether the data could be put to any illegal or inappropriate use;
- How many people are affected;
- What type of people have been affected (pupils, Officers members, suppliers etc) and whether there are wider consequences to the breach.

A clear record should be made of the nature of the breach and the actions taken to mitigate it. The investigation should be completed as a matter of urgency and, wherever possible, within 5 days of the breach being discovered/reported. A further review of the causes of the breach and recommendations for future improvements can be done once the matter has been resolved.

Notification

Some people/agencies may need to be notified as part of the initial containment. However, the decision will normally be made once an investigation has taken place. The DPO/CEO (or nominated representative) should, after seeking expert or legal advice, decide whether anyone should be notified of the breach. In the case of significant breaches, the Information Commissioner's Office (ICO) should be notified. Every incident should be considered on a case by case basis. The following points will help you to decide whether and how to notify:

- Are there any legal/contractual requirements to notify?
- Will notification help prevent the unauthorised or unlawful use of personal data?
- Could notification help the individual – could they act on the information to mitigate risks?
- If a large number of people are affected, or there are very serious consequences, you should notify the ICO. The ICO should only be notified if personal data is involved. There is guidance available from the ICO on when and how to notify them, which can be obtained at: http://www.ico.gov.uk/for_organisations/data_protection/the_guide/~/media/documents/library/Data_Protection/Practical_application/breach_report ing.ashx.
- Consider the dangers of over-notifying. Not every incident warrants notification and over-notification may cause disproportionate enquiries and work.
- The notification should include a description of how and when the breach occurred and what data was involved. Include details of what you have already done to mitigate the risks posed by the breach.
- When notifying individuals, give specific and clear advice on what they can do to protect themselves and what you are willing to do to help them. You should also give them the

opportunity to make a formal complaint if they wish (see the Authority's Complaints Procedure).

Review and Evaluation

Once the initial aftermath of the breach is over, the DPO/CEO (or nominated representative) should fully review both the causes of the breach and the effectiveness of the response to it. It should be written and sent to the next available Management Team meeting for discussion. If systemic or ongoing problems are identified, then an action plan must be drawn up to put these right. If the breach warrants a disciplinary investigation, the manager leading the investigation should liaise with Human Resources for advice and guidance. This breach procedure may need to be reviewed after a breach or after legislative changes, new case law or new guidance. Consideration should be given to reviewing this breach procedure whenever the data protection policy is reviewed.

Implementation

The DPO/CEO should ensure that Officers are aware of the Data Protection policy and its requirements including this breach procedure. This should be undertaken as part of induction and supervision. If Officers have any queries in relation to the policy, they should discuss this with their line manager or the DPO/CEO.