8. DATA BREACH MANAGEMENT

1. **Purpose**

All organisations that process personal data must ensure it is processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures. It is the individual responsibility of all who use, keep or collect personal data to apply the provisions of Article 5(f) of the General Data Protection Regulation 2016.

All partner organisations signed up to the DiSC must take steps to ensure that shared personal data is kept secure at all times against unauthorised or unlawful loss or disclosure.

This guidance sets out the areas that should be considered by staff and managers in the event of a data or information security breach.

2. **Definitions**

GDPR defines a 'personal data breach' 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.

A data breach may occur when for example:

- hard copy files or records are left unattended, lost or stolen;
- laptops, ipads, phones, data sticks or any other removable portable device holding personal or sensitive data are lost or stolen;
- databases or case file management systems are accessed by unauthorised users – either accidentally due to inadequate system access controls or intentionally by hackers;
- equipment fails;
- sensitive information is posted, faxed or emailed to the wrong recipient;
- inappropriate information is released as part of a Subject Access Request;
- unforeseen circumstances such as a fire or flood damage storage or buildings;
- information is obtained by deceiving the person who holds it – blagging offences;
- information is obtained by eavesdropping to phone calls, viewing pc screens in unprotected public spaces - shoulder surfing.

3. **Data breach investigation**

Organisations should have an agreed process for responding to and investigating suspected or actual data breaches which will involve the Information Governance (IG) lead.

8. DATA BREACH MANAGEMENT

Where information is shared between organisations, the Personal Information Sharing Agreement (PISA) should state which organisation will lead the investigation in the event of the loss of shared data.

Each incident of data loss will require a subtly different response plan however, there are four important elements to any breach management plan:

- containment and recovery;
- data sensitivity risk assessment;
- notification/reporting of breach;
- response, evaluation and review.

4. **Containment and recovery**

The investigator should establish who needs to be made aware of the breach and inform them of what they are expected to do to assist in the containment exercise. In all cases, the affected organisation's IG leads should be informed. They will take responsibility for:

- notifying key people within their own organisations, which might include the SIRO, legal teams, ICT security leads, communications team;
- liaison with the Information Commissioner's Office (ICO) and the data subject/s where appropriate.

The investigator should establish whether anything can be done to recover any losses and to limit the damage caused by the breach. In all cases, attempts should be made to recover the information - it is not acceptable to rely on someone who has inadvertently received or found the information to destroy or return it.

It may be appropriate to consider informing the police depending upon the nature of the information that has been lost.

5. **Data sensitivity risk assessment**

To understand the impact of a data breach, the extent of potential damage, and to agree an appropriate course of action, it is helpful to undertake a data sensitivity risk assessment.

The assessment should consider the following:

- what type of information is involved?
- how sensitive is it? Some information is sensitive because of its very personal nature (health records) whilst other information is sensitive because of what might happen if it is misused (bank account details);
- if information has been lost or stolen, is there any protection in place such as encryption?
- what has happened to the information? If information has been stolen, it could be used for purposes which are harmful to the individuals to whom the information relates; if it has been damaged, this poses a different type and level of risk;

- what could the information tell a third party about the individual? Sensitive information could mean very little to an opportunistic laptop thief while the loss of apparently trivial snippets of information could help a determined fraudster build up a detailed picture of other people;
- how many people are affected by the breach? It is not necessarily the case that the bigger risks will accrue from the loss of large amounts of information but is certainly an important determining factor in the overall risk assessment;
- who are the individuals whose information has been lost, damaged or stolen? Whether they are staff, customers, clients or suppliers will to some extent determine the level of risk posed by the breach and, therefore, the actions in attempting to mitigate those risks;
- what harm can come to those individuals? Are there risks to physical safety for example if an individual is fleeing from domestic abuse? Or risks to reputation, or the possibility of financial loss or a combination of these and other aspects of their life? If individuals' bank details have been lost, consider contacting the banks for advice on anything that can be done to help prevent fraudulent use;
- are there wider consequences to consider such as a risk to public health or loss of public confidence in an important service?

6. **Notification/reporting of breach**

Notification obligations are contained in Recitals 85 & 86 and Articles 33 & 34 of GDPR

Notification has a clear purpose, it may:

- enable individuals who may have been affected to take steps to protect themselves;
- ask third parties such as the police, insurers, bank or credit card companies to assist in reducing risks;
- allow the appropriate internal departments to change working practices, perform duties more securely, provide advice and deal with complaints.

The following prompts will help determine if it is appropriate to notify individual data subjects (or owners):

- are there any legal or contractual requirements for notification or sector specific regulators that require notification?
- will notification help meet security obligations with regard to the seventh data protection principle?
- can notification help the individual? Could individuals act on the information you provide to mitigate risks, for example by cancelling a credit card or changing a password?
- if a large number of people are affected, or there are very serious consequences, seek advice about informing the Information Commissioners Office (ICO) from your Information Governance lead;
- consider how notification can be made appropriate for particular groups of individuals, for example, if you are notifying children or vulnerable adults;
- consider the dangers of 'over-notifying'. Not every incident will warrant notification and notifying a whole 2 million strong customer base of an issue

affecting only 2,000 customers may well cause disproportionate enquiries and work.

Include in the notification at least the following:

- describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
- communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;
- describe the likely consequences of the personal data breach;
- describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

7. **Response, evaluation and review**

It is important not only to investigate the causes of the breach but also to evaluate the effectiveness of the response.

A full report should be prepared by the investigator, authorised by a service manager and lodged with the IG lead. This should provide assurance to service users, management and the ICO on the organisations' commitment to information security.