TILLSIDE PARISH COUNCIL

Website: **http://www.tillside.uk/**

Checklist of what to include in a security incident response policy.

A. A data breach of any size is a crisis management situation, which could put an entire council at risk. Data security is not an IT issue, it is an organisational risk, and breach response should involve people from a number of roles across the council.

B. Planning for a breach is therefore essential; every council should have in place a breach response plan, and should designate, in advance, a breach response team which can be convened at short notice to deal with the crisis.

C. Understanding the issues that arise in a breach situation, and practising managing a breach, are essential to effective breach response. Failure to plan and practise increases the regulatory, litigation and reputation risk to the entire council.

D. The checklist below sets out the key issues which a council should consider in preparing for a data breach.

1. The breach response plan

(a) Do you know who should be notified within the council if there is a data breach?

(b) What happens if one of your team in (a) above is away on holiday or otherwise absent. Is there a back-up plan?

(c) Do you have clear reporting lines and decision-making responsibility?

(d) Do you understand what external assistance you might need, with providers in place in advance?

(e) Do you have designated person(s) responsible for managing breaches, with full decision-making authority?

(f) Do you have processes for triaging incidents, identifying actual breaches and activating the breach response team?

(g) Is your breach response plan up to date?

(h) Have you tested your breach response plan?

2. Legal issues

(a) Do you have a process for maintaining legal privilege and confidentiality?

(b) Can you pause document destruction processes?

(c) Do you have appropriate evidence gathering capability, so you can collect information about the breach?

(d) Do you know who your specialist external lawyers who can manage the investigation and give legal advice are?

(e) Do you have a process for managing and logging steps taken in the investigation?

(f) Do you understand your contractual rights and obligations with third parties?

(g) Can you quickly identify third parties you may need to notify?

(h) Do you have appropriate contractual rights to be notified of breaches by third parties?

(i) Do you know how to contact the Information Commissioners Office ("ICO") and with law enforcement who you can involve quickly if necessary?

(j) If you hold credit/ debit card data, do you need to notify your payment processor?

(k) Do you need advice on the legal options available to quickly gather evidence from third parties?

(l) Do you understand your potential liabilities to third parties?

(m) Can you gather information about the breach including taking statements from staff members or councillors who might have seen unusual activity?

(n) Do you understand when you should consider notifying data subjects and / or regulators?

3. Forensic IT

(a) Do you have access to qualified forensic IT capability, either internally or externally?

(b) Do you understand the basic IT do's and don'ts of responding to data breaches?

(c) Do you have an asset inventory to help you identify potentially compromised devices, where those devices are and in whose possession?

(d) Do you understand how data flows in your council, in practice?

(e) Can you quickly secure and isolate potentially compromised devices and data, without destroying evidence?

(f) Can you quickly ensure physical security of premises?

4. Cyber breach insurance

(a) Do you have cyber breach insurance, or other insurance which may cover a data breach?

(b) Do you understand the process for (a) notifying breaches and (b) obtaining consent for actions from insurers?

(c) Do you have emergency contact details for your brokers?

5. Data

(a) Do you know what data you hold (and what you shouldn't hold)?

(b) Is your data appropriately classified?

(c) Do you have, and apply, data destruction policies?

(d) Do you know what data is encrypted, how it is encrypted, and when it may be unencrypted on your systems?

(e) Do you have regularly check you are complying with your retention policy to ensure you are storing only the data you should be?

(f) Do you have appropriate additional protection for sensitive data?

(g) Do you have data loss prevention or similar tools?

(h) Do you understand your logs, how long you retain them for and what they can (or cannot) tell you?

(i) Do you have appropriate logging of staff/ councillor access to data?

6. Data subjects

(a) Do you understand when you should consider notifying data subjects?

(b) Do you understand the contractual and legal rights of data subjects?

(c) Can you quickly prepare appropriately worded notifications to data subjects?

(d) Do you understand the potential harm to data subjects of loss of the different types of data that you hold?

(e) Do you have the ability to appropriately triage and deal with a breach?

(f) Are councillors and staff appropriately trained as to how to deal with data subjects in a breach scenario?

7. Public Relations ("PR")

(a) Do you have access to PR capability experienced in dealing with data breaches?

(b) Do you have template pro-active and re-active press statements?

(c) Can you actively monitor social media after a breach?