

STAPLOE PARISH COUNCIL

Data Security / Breach 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.
 - Examples of personal data breaches and steps to avoid them include:
 - Emails and attachments being sent to the wrong person, or several people – it is easy to click the wrong recipient. Slow down, check thoroughly before clicking 'send'.
 - The wrong people being copied in to emails and attachments. – Use BCC (Blind Carbon Copy) where necessary.
 - Lost memory sticks which contain unencrypted personal data – The council should put protocols in place for memory stick usage.
 - Malware (IT) attach – ensure up to date anti-virus software is in place.
 - Equipment theft – check security provisions.
 - Loss of personal data which is unencrypted

1. The breach response plan

- (a) The Clerk, and Parish Councillors should be notified if there is a data breach.

When a personal data breach has occurred, we 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 eg. the data breach could lead to identity theft, financial loss or physical or emotional harm then we must notify the ICO and the data subject as soon as possible and within 72 hours of its discovery; if it's unlikely eg. we sent an e-mail to the wrong person in the village and there was nothing sensitive in the e-mail then we don't have to report it to the ICO but we should inform the data subjects. However, if we decide we don't need to report the breach, we need to be able to justify this decision, so we should document it. ALWAYS inform the Clerk and councillors of a breach. In assessing risk to rights and freedoms, it's important to focus on the potential negative consequences for individuals

- (b) If one of our team in (a) above is away on holiday the remaining members of the Council will respond.
- (c) Reporting lines would be that all members of the Council / Clerk would inform all other members of the Council / Clerk. If present, the Clerk would then inform the ICO if necessary (see a above). If the Clerk is absent then the Chairman or Vice Chairman would contact the ICO. Call the ICO on 0303 123 1113 to report a breach.
- (d) We may need external assistance from:
 - (i) For website or e-mail security breaches contact Cloudnext on **0333 202 1032**
 - (ii) Providers of the relevant operating system eg. Microsoft for Windows PC breaches. <https://support.office.com/home/contact>
 - (iii) The police for theft of documents or computing equipment. Call 101 and ask for Bedfordshire police.
 - (iv) The ICO 0303 123 1113

STAPLOE PARISH COUNCIL

- (v) If digital forensics are needed contact Sector Forensics on 0845 838 7926 or similar digital forensic company.
- (e) The Parish Clerk is responsible for managing data breaches with decision making authority.
- (f) Councillors and the Clerk would know how to recognise and identify breaches as part of their internal data protection training and they are aware of how to activate the breach response through this policy.
- (g) We keep this plan up to date by reviewing and updating it every year in July or as changes occur (whichever is sooner).
- (h) We have not tested our breach response plan as we are a very small council so it would not be difficult to report a breach.

2. The notification to the ICO referred to in paragraph 1.a. shall at least:

- (a) describe the nature of the personal data breach including where possible, the categories (eg. members of the public, volunteers or Councillors) and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
- (b) communicate the name and contact details of the Clerk or other contact point where more information can be obtained;
- (c) describe the likely consequences of the personal data breach;
- (d) 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. Eg. advising affected members of the public to change e-mail or banking passwords.
- (e) Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.
- (f) The controller shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the supervisory authority to verify compliance with this Article.
- (g) Where there has been a digital breach don't:
 - (i) Discuss the incident with others unless directed
 - (ii) Shut down, power off or back up affected computers
 - (iii) Remotely access affected systems eg. access your e-mail from the web on another device
 - (iv) Use common privileged domain credentials eg. the Council Onedrive folders
 - (v) Delete any files or folders – you might destroy evidence
 - (vi) Install or execute any software on the systems
 - (vii) Conduct anti-virus or similar scanning processes
 - (viii) Attempt to retaliate against perpetrators

STAPLOE PARISH COUNCIL

3. Cyber breach insurance

- (a) The Council are insured by BHIB. Emergency contact details for BHIB are as follows:

Policy number: LCO02558

Tel. 0330 024 0606

BHIB Limited AGM House 3 Barton Close Grove Park Enderby Leicester LE19 1SJ

We are not currently covered for Data Breach Response. We await quote for this but it is expected to be around £50 extra.

4. Data

- (a) See SPC Data Audit Questionnaire for data we hold and Staploe Parish Council Retention Policy (which also specifies how data will be deleted / destroyed).
- (b) Sensitive data such as data consisting of racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data, data concerning health or data concerning a natural person's sex life or sexual orientation (where kept) is categorised by storing it in an e-mail or computer / paper folder marked confidential.
- (c) Data held on the Clerk's external hard drive is encrypted. Data is only transferred between devices using encrypted memory sticks / external hard drives.
- (d) We check we are complying with our retention policy every year in July
- (e) All Councillors and the Clerk have access to all Council data
- (f) Logs of data processing activities are kept in files named "SPC Schedule of Processing (activity name)"

5. Data subjects

- (a) If there is risk of harm (see 1a) to data subjects they should be notified as soon as possible or within 72 hours.
- (b) Harm may be identity theft, emotional distress, financial loss.
- (c) Data subjects should be notified using the following template:
- (d) [DATE] Dear [INDIVIDUAL NAME]:

We (value your business – Hamlets Voice advertisers) and respect the privacy of your information, which is why, as a precautionary measure, we are writing to let you know about a data security incident that [may involve/involves] your personal information. [[Between/On] [IDENTIFY TIME PERIOD OF BREACH], [SUMMARIZE BREACH INCIDENT].] The data accessed [may have included/included] personal information such as [IDENTIFY TYPES OF PERSONAL INFORMATION AT ISSUE]. [To our knowledge, the data accessed did not include any [IDENTIFY TYPES OF PERSONAL INFORMATION NOT INVOLVED]].

This policy was published in May 2018, reviewed in July 2019 and updated in July 2022 with new insurance details.