STOKESLEY TOWN COUNCIL

STOKESLEY TOWN COUNCIL

SECURITY INCIDENT POLICY

LOCAL COUNCIL AWARD SCHEME FOUNDATION

Adopted 12 February 2019

Document Version Control

Version Number	Comments	Date
0.1	Final Draft for Approval	19 January 2019
1.0	Document Approved by Town Council Meeting	12 February 2019

Contents

1. Introduction

This policy specifies the actions to be taken by Stokesley Town Council members and employees with respect to breaches of personal data.

2. What is a breach?

A **personal data breach** means 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 the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.

Examples of personal data breaches include:

- access by an unauthorised third party;
- deliberate or accidental action (or inaction) by a controller or processor;
- sending personal data to an incorrect recipient;
- computing devices containing personal data being lost or stolen;
- alteration of personal data without permission;
- and loss of availability of personal data

3. Dealing with an incident

a) Reporting Point

On discovery of an incident either as a result of automatic notification, accidental discovery, manual record checking or any other means, all personnel will;

- Report the incident to the clerk or assistant clerk of the council by email to **stokesleytc@gmail.com**
- Follow up the email report with a telephone call to the clerk or assistant clerk on 01642 710270.
- If neither the clerk nor the assistant clerk is available inform the chair of the council (contact details available through the website www.stokesleytowncouncil.gov.uk or at the Town Hall).
- If the chair is not available then inform the vice chair (contact details available through the website – www.stokesleytowncouncil.gov.uk or at the Town Hall)

b) Reporting Point Responsibilities

All incidents must be recorded. The clerk or assistant clerk will perform the following actions:

- Note the time, date and nature of incident together with a description and as much detail as appropriate on an Incident Response Form.
- Ensure the protection of any evidence and that a documented chain of evidence is maintained.
- Liaise with relevant authorities, individuals and the media where appropriate.

- Keep a note of all communications together with their date, time, who has been communicated with, and what the content and nature of communication was on the Incident Response Form.

4. Incident Response Plan

- Assess the risk to individuals as a result of a breach: The following must be considered:
- the categories and approximate number of individuals concerned, and;
- the categories and approximate number of personal data records concerned, and;
- the likely consequences of the personal data breach, in particular consider if the impact results is a risk to the rights and freedoms of individuals.
- To help assess the risks refer to the Information Commissioner Office (ICO) website:
  i. https://ico.org.uk/for-organisations/report-a-breach/
  ii. https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/

a) Notifiable Incident

If the incident is deemed to be a **notifiable incident** the following actions must be taken **within 72 hours** of becoming aware of the incident (even if not aware of all the details yet):

Call the Information Commissioners Office on 0303 123 1113 – and provide the following information:

- what has happened;
- when and how the council found out about the breach;
- the people (how many) that have been or may be affected by the breach;
- what the council are doing as a result of the breach; and
- who else has been told

For reporting a breach outside normal working hours use the ICO Reporting Form: https://ico.org.uk/for-organisations/report-a-breach/personal-data-breach/

b) High Risk Incident

If the incident is deemed to result in a **high risk** to the right and freedoms of individuals:

- Within 48 hours the affected individuals must be informed by telephone, letter or email about the incident as there may be a need for them to take actions to mitigate immediate risk of damage to them.
- The individuals must be told in clear and plain language: i. the nature of the personal data breach and;
- A description of the likely consequences of the personal data breach; and
- A description of the measures taken, or proposed to be taken, to deal with the personal data breach and including, where appropriate, of the measures taken to mitigate any possible adverse effects, and;
- The name and contact details of the clerk and chairman from where more information can be obtained;

c) Incident Not Deemed to be Notifiable

If the incident is **not deemed to be notifiable**:

- Update the Incident Response Form along with the outcome of the risk assessment.
- Include the steps and evidence used to identify and classify the risk. Include reasons why the incident is not deemed to result in a risk to the rights and freedoms of individuals.

5. Incident Review

The council clerk and chairman will ensure that the incident is reviewed at the next appropriate Council meeting under the Policy and Security section of the agenda.

a. The Council will consider whether discussion of the incident warrants exclusion of the press and public from the meeting during that discussion.
b. The Council will determine if there are any further actions that need to be assigned or completed as a result of the incident.
c. The Council may decide to refer further actions to a committee, working group or external parties.

This final stage of the incident may require a review of this policy document.

6. Policy Review

This policy will be reviewed annually or at any other time the council deems necessary.

Appendix 1 – Incident Report Form

The following is a copy of the form to be completed taken from the following source:

https://ico.org.uk/for-organisations/report-a-breach/personal-data-breach/

The report to the ICO should be made by downloading the original form from this link.

ico. Information Commissioner's Office

Report a personal data breach

This form is for organisations that have experienced a personal data breach and need to report it to the ICO. Please do not include any of the personal data involved in the breach when completing this form. For example, do not provide the names of data subjects affected by the breach. If we need this information, we will ask for it later.

You should ensure the information provided is as accurate as possible and supply as much detail as possible.

If you have already spoken to a member of ICO staff about this breach, please give their name:

Report type

- ○ Initial report
- ○ Follow-up report

(Follow-up reports only) ICO case reference:

Reason for report – after consulting the guidance

- ○ I consider the incident meets the threshold to report
- ○ I do not consider the incident meets the threshold to report, however I want you to be aware
- ◉ I am unclear whether the incident meets the threshold to report

About the breach

What has happened?

Tell us as much as you can about what happened, what went wrong and how it happened.

Was the breach caused by a cyber incident?

- ○ Yes
- ○ No
- ○ Don't know

How did you find out about the breach?

When did you discover the breach?

Date:

Time:

When did the breach happen?

Date:

Time:

Categories of personal data included in the breach (tick all that apply)

- ☐ Data revealing racial or ethnic origin
- ☐ Political opinions
- ☐ Religious or philosophical beliefs
- ☐ Trade union membership
- ☐ Sex life data
- ☐ Sexual orientation data
- ☐ Gender reassignment data
- ☐ Health data
- ☐ Basic personal identifiers, e.g. name, contact details
- ☐ Identification data, e.g. usernames, passwords
- ☐ Economic and financial data, e.g. credit card numbers, bank details
- ☐ Official documents, e.g. driving licences
- ☐ Location data
- ☐ Genetic or biometric data
- ☐ Criminal convictions, offences
- ☐ Not yet known
- ☐ Other (please give details below)

Number of personal data records concerned?

How many data subjects could be affected?

Categories of data subjects affected (tick all that apply)

- [ ] Employees
- [ ] Users
- [ ] Subscribers
- [ ] Students
- [ ] Customers or prospective customers
- [ ] Patients
- [ ] Children
- [ ] Vulnerable adults
- [ ] Not yet known
- [ ] Other (please give details below)

Potential consequences of the breach

Please describe the possible impact on data subjects, as a result of the breach. Please state if there has been any actual harm to data subjects

What is the likelihood that data subjects will experience significant consequences as a result of the breach?

- ○ Very likely
- ○ Likely
- ○ Neutral - neither likely nor unlikely
- ○ Unlikely
- ○ Very unlikely
- ○ Not yet known

Please give details

(Cyber incidents only) Has the confidentiality, integrity and/or availability of your information systems been affected?

- ○ High - you have lost the ability to provide all critical services to all users
- ○ Medium - you have lost the ability to provide a critical service to some
- ○ Low - there is no loss of efficiency, or a low loss of efficiency, and you can still provide all critical services to all users
- ○ Not yet known

(Cyber incidents only) If you answered yes, please specify (tick all that apply)

- ☐ Confidentiality
- ☐ Integrity
- ☐ Availability

(Cyber incidents only) Impact on your organisation

- ○ Yes
- ○ No
- ○ Don't know

(Cyber incidents only) Recovery time

- ○ Regular - you can predict your recovery time, with existing resources
- ○ Supplemented - you can predict your recovery time with additional
- ○ Extended - you cannot predict your recovery time, and need extra resources
- ○ Not recoverable - recovery from the incident is not possible, eg backups can't be restored
- ○ Complete - recovery is complete
- ○ Not yet known

Had the staff member involved in this breach received data protection training in the last two years?

- ○ Yes
- ○ No
- ○ Don't know

(Initial reports only) If there has been a delay in reporting this breach, please explain why

(Follow-up reports only) Describe any measures you had in place before the breach with the aim of preventing a breach of this nature*

Taking action

Describe the actions you have taken, or propose to take, as a result of the breach

Include, where appropriate, actions you have taken to fix the problem, and to mitigate any adverse effects, e.g. confirmed data sent in error has been destroyed, updated passwords, planning information security training.

(Follow-up reports only) Outline any steps you are taking to prevent a recurrence, and when you expect they will be completed*

Have you told data subjects about the breach?

- Yes, we've told affected data subjects
- We're about to, or are in the process of telling data subjects
- No, they're already aware
- No, but we're planning to
- No, we've decided not to
- We haven't decided yet if we will tell them or not
- Something else (please give details below)

Have you told, or are you planning to tell any other organisations about the breach?

e.g. the police, other regulators or supervisory authorities. In case we need to make contact with other agencies

- Yes
- No
- Don't know

If you answered yes, please specify

About you

Organisation (data controller) name

Registered organisation address

Person making this report

In case we need to contact you about this report

Name:

Email:

Phone:

Data protection officer

Or the senior person responsible for data protection in your organisation

☐ Same details as above

Name:

Email:

Phone:

Sending this form

Initial report

If this is your initial report, please send your completed form to casework@ico.org.uk, with 'Personal data breach notification' in the subject field.

Follow up report

If this is a follow up report, please *reply to the email we sent you*, attaching this completed form to it. (Make sure you leave the subject line as it is – this will ensure your follow-up gets added to your case).

OR, send by post to:

The Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

Please note that we cannot guarantee security of forms or any attachments sent by email.

What happens next?

You should read our guidance to determine what steps you should take.

Based on the information you have provided, we will contact you within seven calendar days to provide information about our next steps. If this is your initial report, we'll give you a case reference number. If we consider the incident is minor or you have indicated that you do not consider it meets the threshold for reporting, you may not receive a response from us.

If your correspondence relates to an existing case, we'll add it to your case for your case officer to consider.

If you need any help in completing this form, please contact our helpline on 0303 123 1113 (operates 9am to 5pm Monday to Friday).

For information about what we do with personal data see our privacy notice.