Fakenham Connect
Oak Street
Fakenham
Norfolk
NR21 9DY
Tel: 01328 853653
e-mail: info@fakenhamtowncouncil.gov.uk
website: fakenhamtowncouncil.gov.uk

Fakenham Town Council

DATA BREACH PROCEDURE

DOCUMENT INFORMATION

CLASSIFICATION		VERSION NUMBER	0.1	STATUS	DRAFT
VALID FROM		APPROVED BY		PREPARED BY	Bulletproof

VERSION HISTORY

DATE	VERSION NUMBER	NAME	CHANGE DESCRIPTION
04/05/2025	V0.1	Bulletproof	Initial Document Creation

1. INTRODUCTION

A data breach procedure creates a framework for all staff at Fakenham Town Council who hold and processes personal data in relation to employees, members and contractors. As a council we pride ourselves on the security and lawful handling of personal data including special category data. At Fakenham Town Council we process data in accordance with the relevant legal requirements, namely General Data Protection Regulation 2016/679; the UK Data Protection Act 2018 and all relevant EU and UK data protection legislation. As a council we ensure that care is taken to protect personal data from incidents (either committed accidentally or deliberately) and to avoid a data breach that could compromise security. Any compromise to the confidentiality, integrity, or availability of information we hold, in terms of breach of may result in harm to individual(s), reputational damage, a detrimental effect on service provision, amount to legislative noncompliance, and/or financial costs.

2. DEFINITION OF DATA BREACH

A personal data breach is defined as a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity, or availability of personal data. In short, there will be a personal data breach whenever any personal data is lost, destroyed, corrupted, or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable, for example, when it has been encrypted by ransomware, or accidentally lost or destroyed.

Personal data breaches can include:

- Loss or theft of personal data and/or equipment on which data is stored

- 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
- Loss of availability of personal data
- Hacking attack
- Cyber attack
- Equipment failure
- Human error
- Unforeseen circumstances such as a fire or flood
- Flawed data destruction procedures.

3. RESPONSIBILITIES

Fakenham Town Council recognises that it has responsibility to ensure that all Fakenham Town Council data is processed in accordance with any relevant legislation and guidance to which it is subject to.

All individuals covered by the scope of this policy are responsible for reporting actual, suspected, threatened or potential data breaches and for assisting with investigations as required, particularly if urgent action must be taken to prevent any or further damage.

The Clerk is responsible for drawing up guidance on access to information, including data protection and promoting compliance with this policy in such a way as to ensure the easy, appropriate and timely management of incidents.

Failure to comply with the policy may result in an administrative fine for Fakenham Town Council by the information commissioner's office (ICO) and/or disciplinary action against individuals under Fakenham Town Council procedures.

4. PERSONAL DATA BREACH NOTIFICATION: GENERAL POINTS

When a personal data breach is suspected, it is the responsibility of the employee or Councillor who identifies the breach to report this to the Clerk immediately to ensure the breach can be dealt with within the timescales required.

All data breaches, regardless of their severity and impact will be recorded in the council data breach register.

In the event of a data breach, employees must not speak to third parties or the press without permission from the Clerk. Any questions from third parties related to any suspected or actual data breach should be passed to the Clerk.

If there is doubt as to whether a data breach should be reported to the ICO and/or data subject, the Clerk should seek guidance from the ICO.

5. PERSONAL DATA BREACH NOTIFICATION: DATA CONTROLLER TO SUPERVISORY AUTHORITY

When the personal data breach or suspected data breach affects personal data that is being processed by Fakenham Town Council as a data controller, the following actions are performed by the Clerk:

1) Fakenham Town Council must establish whether the personal data breach should be reported to the Supervisory Authority.

2) In order to establish the risk to the rights and freedoms of the data subject affected, the Clerk must assess the risks in accordance with the guidelines outline in section 9.0 of this document and, where required, using the ICO tool here.

3) The Supervisory Authority must be notified (see here) with undue delay but no later than in 72 hours, if the personal data breach is likely to result in a risk to the rights and freedoms of the data subjects affected by the personal data breach.

Any possible reasons for delay beyond 72 hours must be communicated to the Supervisory Authority. The Clerk will send Notifications to the Supervisory Authority that will include the following:

- A description of the nature of the breach
- Categories of personal data affected
- Approximate number of data subjects affected
- Name and contact details of the Data Breach Response Team Leader/ Data Protection Officer
- Consequences of the personal data breach
- Measures taken to address the personal data breach

6. PERSONAL DATA BREACH NOTIFICATION: DATA CONTROLLER TO DATA SUBJECT

The Clerk must assess if the personal data breach is likely to result in high risk to the rights and freedoms of the data subject in accordance with the guidelines outlined in section 9 of this document. If there is a high risk, Fakenham Town Council must notify, without undue delay, the affected data subjects. The notification to the data subjects must be written in clear and plain language and include:

- The name and contact details of any data protection officer you have, or other contact point where more information can be obtained;
- a description of the likely consequences of the personal data breach; and
- a description of the measures taken or proposed to deal with the personal data breach and, where appropriate, a description of the measures taken to mitigate any possible adverse effects.
- If possible, Fakenham Town Council should give specific and clear advice to individuals on the steps they can take to protect themselves, and what Fakenham Town Council is able to do to help them. Depending on the circumstances, this may include such things as:
  - forcing a password reset;
  - advising individuals to use strong, unique passwords; and
  - telling them to look out for phishing emails or fraudulent activity on their accounts.

If, due to the number of affected data subjects, it is disproportionately difficult to notify each affected data subject, Fakenham Town Council must take the necessary measures to ensure that the affected data subjects are notified by using appropriate, publicly available channels.

7. PERSONAL DATA BREACH NOTIFICATION: DATA PROCESSOR TO CONTROLLER

Where Fakenham Town Council acts as a processor, any data breach identified must be reported, without undue delay to the controller(s) of the personal data. Information relating to relevant controllers of personal data will be found on the Records of Processing Activities (Processor) document. Information to provide to the controller should include:

- The date and time the breach was identified
- A description of the nature of the breach
- Categories of personal data affected
- Approximate number of data subjects affected
- Name and contact details of the Clerk
- Consequences of the personal data breach
- Measures taken to address the personal data breach
- Any mitigating measures the controller needs to take

8. PERSONAL DATA BREACH NOTIFICATION: NOTIFICATION OF OTHER THIRD PARTIES

Fakenham Town Council is responsible for checking with sectoral regulations of the relevant parties that should be notified following a severe data breach. Significant cyber incidents may also need to be reported to the National Cyber Security Centre, more details can be found here.

Data breaches that may lead to individuals being victims of fraud should be reported to Action Fraud the UK's national fraud and cybercrime reporting centre.

It may also be necessary to consider notifying third parties such as the police, insurers, professional bodies, or bank or credit card companies who can help reduce the risk of financial loss to individuals.

9. GRADING THE PERSONAL DATA BREACH

Any incident must be graded according to the significance of the breach and the likelihood of serious consequences occurring. The incident must be graded according to the impact on the individual or groups of individuals and not the organisation.

Likelihood grade	Likelihood of adverse effect	Description
1	Not occurred	There is absolute certainty that there can be no adverse effect. This may involve a reputable audit trail or forensic evidence
2	Not likely or any incident involving vulnerable groups even if no adverse effect occurred.	In cases where there is no evidence that can prove that no adverse effect has occurred this must be selected.
3	Likely	It is likely that there will be an occurrence of an adverse effect arising from the breach.
4	Highly likely	There is almost certainty that at some point in the future an adverse effect will happen.
5	Occurred	There is a reported occurrence of an adverse effect arising from the breach.

Severity Grade	Severity of the adverse effect on Individuals	Description
1	No adverse effect	There is absolute certainty that no adverse effect can arise from the breach.
2	Potentially some minor adverse effect or any incident involving vulnerable groups even if no adverse effect occurred.	A minor adverse effect must be selected where there is no absolute certainty. A minor adverse effect may be sending an email containing personal data about an employee to the wrong recipient.
3	Potentially some adverse effect.	An adverse effect may be release of confidential information into the public domain leading to embarrassment.
4	Potentially Pain and suffering/ financial loss.	There has been reported suffering and decline in health arising from the breach or there has been some financial detriment occurred. A person is at risk of harassment or violence from exposed information.
5	Death/ catastrophic event.	A person dies or suffers a catastrophic occurrence. Specific risk information for tailored response is wrong or not available.

9.1 BREACH ASSESSMENT GRID

This operates on a 5 x 5 basis with anything other than “grey breaches” being reportable. Incidents where the grading results are in the red are advised to notify data subjects.

s

Severity (Impact)	Catastrophic	5	5	10	15	20	25
	Serious	4	4	8	12	16	20
	Adverse	3	3	6	9	12	15
	Minor	2	2	4	6	8	10
	No adverse effect	1	1	2	3	4	5
			1	2	3	4	5
			Not Occurred	Not Likely	Likely	Highly Likely	Occurred
			Likelihood that citizens' rights have been affected (harm)				