Chippenham Town Council | Improving the quality of town life

Data Breach Management Procedure

Chippenham Town Council

Approved and adopted by:
Strategy and Resources Committee

Date policy was adopted: 13.06.18

Review date: 13.06.21

Updates

Amendments which do not require a policy review

Date:

Detail:

Contents

1		**Change Control**	**4**
2		**Definitions**	**5**
3		**Mission Statement**	**6**
	3.1	Purpose	6
4		**Spidergram of Policies**	**7**
5		**Identifying a Breach**	**8**
6		**Containment and Recovery**	**9**
7		**Assessment of Ongoing Risk**	**11**
	7.1	Risk Definition	11
8		**Notification of Breach**	**12**
	8.1	To the ICO	12
	8.2	To the data subject	13
	8.3	Notification Requirements Flowchart	14
9		**Evaluation and Response**	**15**
10		**Training & Development**	**16**
11		**Further Information**	**17**
Annex 1 – Data Incident Information			**18**

1 Change Control

This Policy was created in	May 2018
Council Staff were consulted on this document and it was accepted on	
It was ratified by the Council on	
Renewal data	April 2019
This version is	Version 1.0
It replaces	No previous version
It is necessary to comply with	Data Protection Act 1998 General Data Protection Regulation 2016

2 Definitions

Data Protection Act 1998 ("DPA")	The law on data protection in the UK
General Data Protection Regulation ("GDPR")	A new law on data protection that comes into force on 25 May 2018 throughout Europe
Data Controller	A person or organisation that handles and processes personal data and determines the way such data should be processed
Personal Data	Any information from which a living individual can be identified
Sensitive Personal Data	Any Personal Data which includes further information as defined in the DPA. Further information includes (i) racial or ethnic origin; (ii) political opinions; (iii) religious beliefs; (iv) membership of a trade union; (v) physical or mental health or condition; (vi) sexual life or preferences; (vii) information about any criminal offence or court proceedings related to a criminal offence
Information Commissioner's Office ("ICO")	The statutory regulator of the DPA and the GDPR
Privacy Notice	A description of Personal Data held by the Council, along with details of purpose, retention and other information about how the Council will handle the Personal Data
Data Subject	As defined in the DPA and the GDPR. The Data Subject is the person who the Personal Data is about, or who is identified by the Personal Data

3 Mission Statement

Chippenham Town Council ("the Council") is a town council representing the local community, delivering services to meet local needs and improving the quality of town life for all.

In order to make this happen, the Council collects and uses Personal Data about residents, staff, volunteers, councillors and other individuals who all play their part in being part of the community. This information is gathered in order to enable the Council to provide a rich and broad service. In addition, there may be a legal requirement to use information for the purpose of sharing it with other organisations. In some cases, the Council must collect information to ensure that it complies with statutory obligations.

The Council holds large amounts of personal and sensitive data. It is responsible for safeguarding the data it holds and is legally bound under the GDPR to ensure the security and confidentiality of personal information processed. These responsibilities extend to other organisations working on behalf of the Council.

In the unlikely event of a breach, it is vital that appropriate action is taken to minimise any associated risk as soon as possible. The Council is committed to ensuring that should a breach have an impact on an individual, a strong and quick internal reporting mechanism can ensure that any impact is at an absolute minimum. The need to report quickly is also good practice.

3.1 Purpose

The Council strives to ensure that personal information is dealt with correctly and securely and in accordance with the GDPR and related legislation such as the DPA.

The GDPR introduces for the first time a legal requirement for a breach of personal data to be reported to the ICO and, in certain cases, communicate the breach to the data subject(s) affected by the breach.

Principle 7 of the DPA states as follows:

Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal information and against accidental loss or destruction of, or damage to, personal information.

Accordingly, this Policy is an essential part of the Council's compliance with the GDPR and Principle 7.

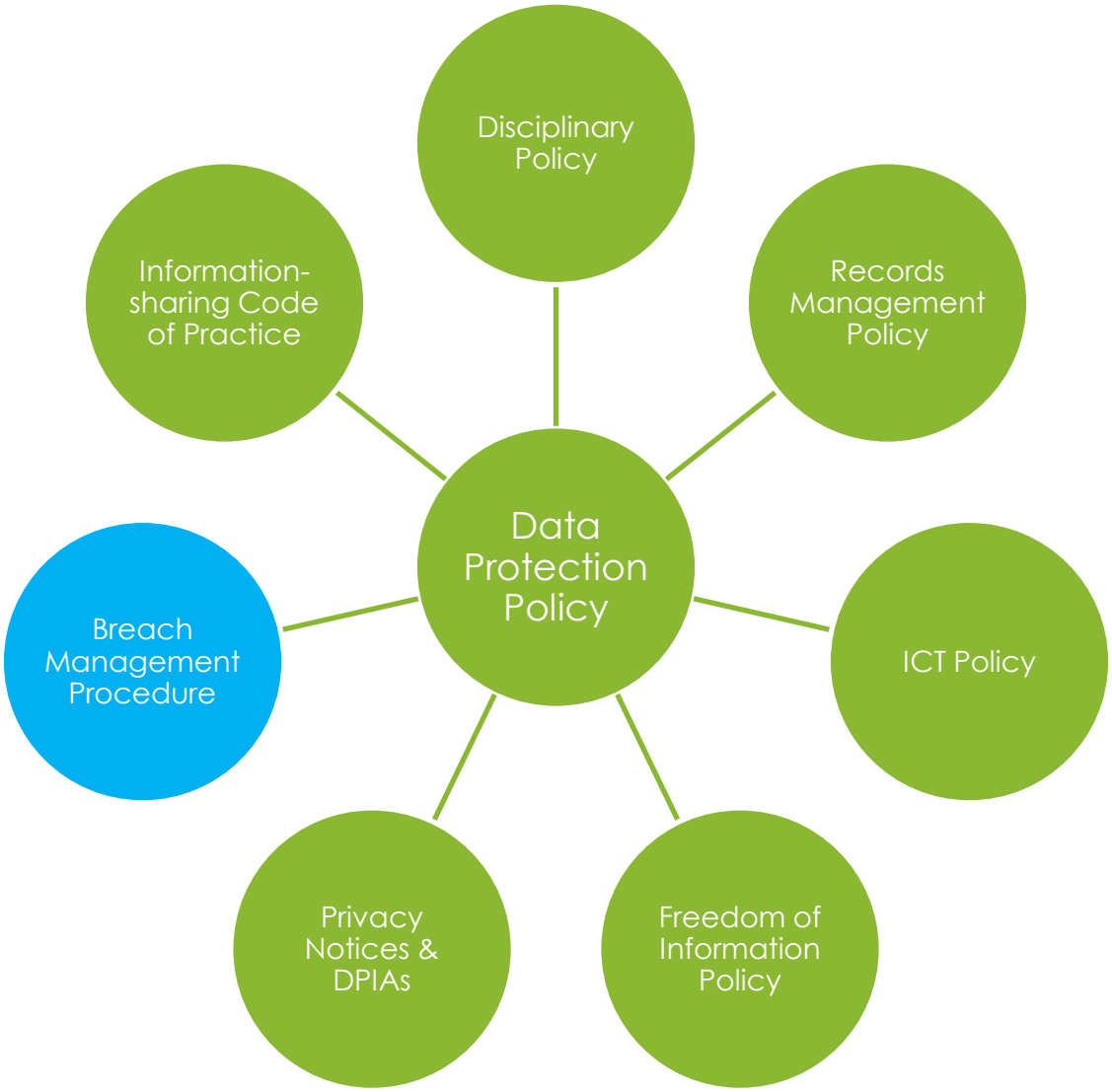
All staff involved with the collection, processing and disclosure of personal data will be aware of their duties and responsibilities by virtue of the Council's Data Protection Policy.

The spidergram overleaf shows how this Policy interacts with the Data Protection Policy and policies.

Staff are expected to adhere to the principles and spirit of this Policy in order to protect Personal Data belonging to our residents, friends of the Council and other members of staff. Anyone found to have breached this Policy may find that the Council will invoke the Disciplinary Procedure.

This Policy has been approved by the Council, and is evidence of the commitment the Council makes to safeguarding Personal Data.

4 Spidergram of Policies



5 Identifying a Breach

The GDPR is clear that a data breach is 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"[1].

What this means is that security incidents, perhaps caused by an IT error or loss of service, may not be a data breach. All personal data breaches will be security incidents, but not all security incidents will be personal data breaches. This Policy is concerned with the former not the latter.

Data breaches can be categorised in the following well-known information security principles:

Confidentiality breach where there is an unauthorised or accidental disclosure of, or access to, personal data

Availability breach where there is an accidental or unauthorised loss of access to, or destruction of, personal data

Integrity breach where there is an unauthorised or accidental alteration of personal data

A breach can be all three at the same time, or any combination of these.

Some of the most common ways in which Personal Data is breached is as follows:

- Loss or theft of data or equipment where data is stored
- Unauthorised use or access to data
- Human error, e.g. Personal information posted incorrectly
- Unforeseen circumstances, e.g. Floods or fires
- Equipment failure
- Circumstances where IT systems are hacked
- Blagging offences or phishing scams where information is obtained by deception

[1] Article 4(12) GDPR

6 Containment and Recovery

The Council requires that anyone who becomes aware of a breach or a potential breach must alert a member of the Senior Management Team immediately.

In addition, staff at the Council and councillors must report any such breach or potential breach to a member of the Senior Management Team immediately, and no later than within 1 hour of becoming aware of a breach. Staff and councillors should use the form annexed to this Procedure to report a breach internally.

Not reporting a breach will most likely mean that the Council's Disciplinary Policy is invoked.

The following process should be followed when a breach is reported:

The Council's key priority during this period is to recover the data and assess the impact of the breach on any data subject. The Council will involve any of the following stakeholders in assisting them to do this:

- Data Protection Officer
- Chief Executive
- Deputy Chief Executive
- Head of Finance and Administration
- Leader of the Council
- Other councillors
- Office/admin staff
- Legal adviser to the Council
- HR adviser to the Council

The DPO will establish the full details of the breach and establish what steps need to be taken to recover any losses and limit damage. This might include:

- The use of back up files to restore lost of damaged data
- The physical recovery of lost equipment
- Shutting down relevant IT systems
- Changing access codes or passwords
- Informing staff, residents and councillors
- Informing the Police if appropriate
- Reporting the breach to the ICO

It is crucial that throughout this period, if it is likely that the breach will impact the safety or wellbeing of any person, that person's interests should be prioritised and deployment of safeguarding procedures is commenced.

7 Assessment of Ongoing Risk

The next stage requires the Council to assess any risks that might arise from the breach. This will help to ascertain what information was or may have been compromised by the breach and any potential adverse effects it might have on any individuals.

The following points will be considered:

- What type and volume of personal data was involved
- How sensitive was the data
- The level of protection of the data, e.g. Encryption
- What has happened to the data. If the data has been stolen, it could be used for purposes which are harmful to the individuals to whom the data relate; if it has been damaged, how might this impact on individuals' lives.
- What the data could tell a third party about the individual. Sensitive personal data could mean very little to an opportunistic laptop thief, whilst the loss of trivial information could help a determined fraudster build up a detailed picture of other people
- How many people are affected by the breach
- What harm may come to the individuals affected by the breach
- What the wider consequences (political/financial/social/educational/legal) of the breach might be

The Data Protection Officer will report any outcomes and proposals to be adopted by SMT, councillors or rolled out to staff as appropriate.

7.1 Risk Definition

Risk is a trigger for notification. The Council needs to assess the risk that could result from data breach as it will determine whether notification is required to the ICO and, if necessary, to the individuals (data subject) concerned.

Risk: Notification to ICO

High Risk: Notification to ICO and Data Subject

8 Notification of Breach

A member of SMT, in conjunction with the Data Protection Officer shall consider whether to notify to any of the following groups:

- The data subject
- The Leader of the Council
- The wider staff group
- The Council community and residents
- The ICO
- The Council's insurers
- The Council's bank
- The Press

Notification should have a clear purpose, and the decision whether to notify should be clearly documented.

Staff will be aware that until such time as a breach is formally published, the nature of the breach itself will be and should remain confidential.

8.1 To the ICO

Notification to the ICO is required if a breach is likely to result in a risk to the rights and freedoms of individuals

The GDPR requires that breaches must be reported to the ICO "without undue delay and, where feasible, not later than 72 hours after having become aware of it"[2].

When is the Council "aware"?

The Council will be aware of a breach when it has a reasonable degree of certainty that a security incident has occurred and which has lead to personal data being compromised.

To have this certainty, the Council may need to investigate facts and circumstances and this is not included in the time period set out above.

What must be reported

The Council must and will provide information to the ICO as set out in the GDPR:

- The nature of the breach including the categorise and approximate number of data subjects concerned
- The contact details of the Data Protection Officer

[2] Article 33(1) GDPR

- The likely consequences of the breach
- The measures taken or proposed to be taken to mitigate possible adverse effects

8.1.1 Exemptions

Notification to the ICO is not required if a breach is unlikely to result in a risk to the rights and freedoms of individuals

Furthermore, if there is no risk to the "rights and freedoms" of any individual, then there is no need to report. An example might be where personal data are already publicly available and a disclosure of such data does not constitute a likely risk to the individual. The Council will assess – in conjunction with its Data Protection Officer – the level to which there is a risk to the rights and freedoms of any individual.

8.2 To the data subject

When the breach is likely to result in a **high** risk to any individual, the Council must also inform that individual "without undue delay"

The same information must be provided as set out above.

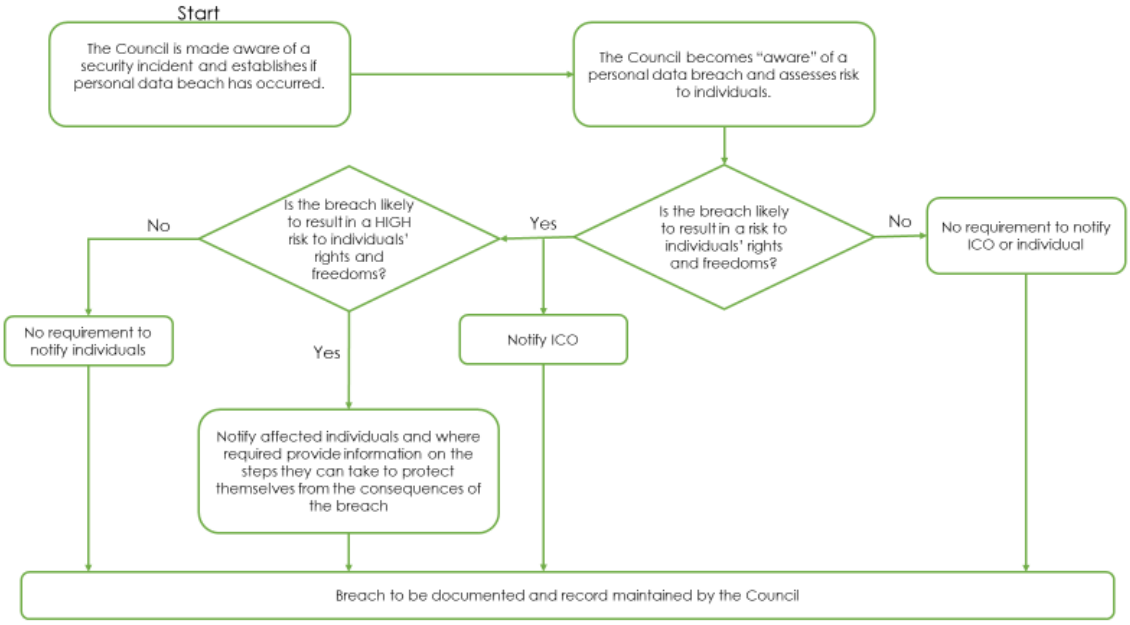
8.2.1 Exemptions

Notification to the individual is not required if a breach is unlikely to result in a high risk to the rights and freedoms of individuals

Notification is not required where:

- The data is encrypted or cannot be accessed or read intelligibly
- The Council has taken steps immediately after the breach to ensure that no risk to any individual can materialise (e.g. It has retrieved the data)
- It would involve a disproportionate effort (e.g. If a large number of people were affected and not all of them are contactable)

8.3 Notification Requirements Flowchart



9 Evaluation and Response

The Council will evaluate and review the cause of the breach and effectiveness of the response to it. This will help reveal any systemic or ongoing problems and prevent any future breaches from occurring.

All breaches will be recorded regardless of whether it needs to be notified to external parties, and the outcomes and decisions made in respect of them must also be recorded.

The Council hopes that data breaches will be an extremely rare occurrence. However, whenever they do happen the Council understands the need to learn any lessons and tighten up security.

In all cases of data breach which involve human error, the staff member involved will be required to undergo refresher data protection training. Further training needs may be identified and rolled out across the Council.

In cases where ICT is an issue the Council will work with its ICT provider to increase security where appropriate.

All Council processes will be reviewed to ensure that there is no scope for a similar data breach to occur.

10 Training & Development

The Council is committed to ensuring the staff adopt the highest standards in relation to the processing and handling of Personal Data.

All existing staff will be trained within 6 months of the dissemination of this Policy.

New staff (and councillors) will be trained as part of their induction within 3 months of their joining the Council and being able to access Personal Data.

Staff will be re-trained according to their needs against the tide of new guidance and legislation. It is anticipated that this will usually be annually.

No member of staff will have access to any Personal Data unless they have read this Policy first.

11 Further Information

Any person reading this Policy requiring further information or assistance is invited to contact the Council's Head of Finance and Administration.

Where any person has a complaint about the way the Council has handled their Personal Data or that of their child's, they may address their concern in writing to the Chief Executive.

For further information about the DPA, GDPR and its application, the Information Commissioner's Office has a wealth of information on its website – www.ico.org.uk

Annex 1 – Data Incident Information

Please return this form to dpo@chippenham.gov.uk and a member of SMT

Data Incident Report Form
Data lost *(Describe the data that has been lost)*
Security of data *(Describe how the data was stored (electronic, encrypted, paper, locked etc.))*
How many individuals have been affected?
Explanation of facts leading to loss *(Describe how the data was lost – give specific details of how/when you realised the data was lost, and what actions you took to recover i)t*
Who lost the data? *(Name and post of staff member or councillor)*
When was it lost? *(Give time and date)*
Where was it lost? *(Give a precise location)*
Who received it?
Give an explanation of any steps taken so far to retrieve the data
Record of action taken
Has the data been recovered/destroyed?
Data Protection training – Have you attended the training, and if so when?
Who else have you notified?