Adopted By The Parish Council : 18th July 2019

Review Date : May 2020

Data Breach Incident Response Policy

1. PURPOSE

The purpose of this policy is to provide a framework for reporting and managing data security breaches affecting personal or sensitive personal data (defined below) held by Dalton Parish Council.

2. WHAT IS A PERSONAL DATA SECURITY BREACH?

A personal data security breach is any event that has the potential to affect the confidentiality, integrity or availability of personal data held by Dalton Parish Council in any format. Examples of personal data security breaches:

- the disclosure of confidential data to unauthorised individuals;
- loss or theft of portable devices or equipment containing identifiable personal, confidential or sensitive data e.g. PCs, USB, mobile phones; Laptops, disks etc.;
- loss or theft of paper records;
- inappropriate access controls allowing unauthorised use of information;
- attempts to gain unauthorised access to computer systems, e.g. hacking;
- viruses or other security attacks on IT equipment systems or networks;
- breaches of physical security e.g. forcing of doors or windows into secure room or filing cabinet containing confidential information;
- confidential information left unlocked in accessible areas;
- insecure disposal of confidential paper;
- leaving IT equipment unattended when logged-in to a user account without locking the screen to stop others accessing information;
- publication of confidential data on the internet in error and accidental disclosure of passwords;
- misdirected emails or faxes containing identifiable personal, confidential or sensitive data.

3. WHAT TYPES OF DATA DO THESE PROCEDURES APPLY TO?

These procedures apply to:

- all personal data created or received by Dalton Parish Council in any format (including paper records), whether used in the workplace, stored on portable devices and media, transported from the workplace physically or electronically or accessed remotely;
- personal data held on all Dalton Parish Council IT systems.
- any other IT systems on which Dalton Parish Council data is held or processed.

4. WHO IS RESPONSIBLE FOR MANAGING PERSONAL DATA SECURITY BREACHES?

Personal data security breaches are managed by the Data Controller, which is the Parish Council.

5. PROCEDURE FOR REPORTING DATA SECURITY BREACHES

In the event of a breach of data security occurring, it is vital to ensure that it is dealt with immediately and appropriately to minimise the impact of the breach and prevent a recurrence.

If a breach or potential or suspected data breach has been reported to you please report this immediately to the Chair of the Parish Council and Clerk.

The data breach document should be completed. This will enable all the relevant details of the incident to be recorded consistently and communicated on a need-to-know basis to relevant personnel so that prompt and appropriate action can be taken to resolve the incident.

Step 1: Identification and initial assessment of the incident

If you are aware that a data security breach has occurred, please report it immediately to the Chair of the Parish Council and Clerk. They should conduct an initial assessment of the incident by establishing:

- if a personal data security breach has taken place; if so:
- what personal data is involved in the breach;
- the cause of the breach;
- the extent of the breach (how many individuals are affected);
- the harms to affected individuals that could potentially be caused by the breach; and
- how the breach can be contained.

Following this initial assessment an appropriate lead investigator will be appointed to investigate the incident.

The Lead Investigator will determine the **severity** of the incident using the reference to the table below and by completing part 2 of the Data Security Breach Report Form. The severity of the incident will be categorised on a scale of 1 to 6. Where incidents are rated 3 or above this will be reported directly to the full Parish Council.

Rating	0	1	2	3	4	5	6
Reputation	No significant reflection on any individual or body Media interest very unlikely	Damage to an individual's reputation. Possible media interest (eg prominent member of the Parish Council involved)	Damage to a department's reputation. Some local or subject specific media interest that may not go public	Damage to a service's reputation/Parish Council member involved. Low key local or media coverage	Damage to Parish Councils reputation/ local media coverage.	Damage to Parish Councils reputation/ national media coverage.	Monetary Penalty Imposed by ICO
Individuals potentially affected	Minor breach of confidentiality. Only a single individual affected	Potentially serious breach. Less than 5 people affected or risk assessed as low (eg files were encrypted)	Serious potential breach & risk assessed high (eg unencrypted sensitive/health records lost) Up to 20 people affected	Serious breach of confidentiality eg up to 100 people affected and/or identifiable or particularly sensitive ie redundancies, restructuring	Serious breach with either particular sensitivity (eg sexual or mental health details, identifying information of vulnerable people), or up to 1000 people affected	Serious breach with potential for ID theft or over 1000 people affected	Restitution to injured parties Other Liabilities Additional Security Legal Costs

Step 2: Containment and Recovery

Once it has been established that a data breach has occurred, the Parish Council needs to take immediate and appropriate action to limit the breach.

The Lead Investigator and relevant staff will:

- Establish who needs to be made aware of the breach
- Establish whether there is anything that can be done to recover any losses and limit the damage the breach can cause
- Establish if it is appropriate to notify affected individuals immediately
- Where appropriate (e.g. in cases involving theft or other criminal activity), inform the police.

Step 3: Risk Assessment

In assessing the risk arising from a data security breach, the relevant stakeholders are required to consider the potential adverse consequences for individuals, i.e. how likely are adverse consequences to materialise and, if so, how serious or substantial are they likely to be. The information provided at Stage 1 on the Data Security Breach Report Form will assist with this stage.

The Lead Investigator will review the incident report to:

- Assess the risks and consequences of the breach:
    - Risks for individuals:
        - What are the potential adverse consequences for individuals?
        - How serious or substantial are these consequences?
        - How likely are they to happen?
    - Risks for the Parish Council:
        - Strategic & Operational
        - Compliance/Legal

- Financial
- Reputational Continuity of Service Levels

- Consider what type of data is involved, how sensitive is it? Were there any protections such as encryption? What has happened to the data? If 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 this poses a different type and level of risk;
- Consider how many individuals' personal data are affected by the breach. It is not necessarily the case that the bigger risks will accrue from the loss of large amounts of data but is certainly an important determining factor in the overall risk assessment;
- Consider the individuals whose data has been breached.
- Consider what harm can come to the affected individuals. Are there risks of physical safety or reputation, of financial loss or a combination?
- Consider if there are wider consequences to consider such as a loss of public confidence in a service the Parish Council provides;
- Determine, where appropriate, what further remedial action should be taken on the basis of the incident report to mitigate the impact of the breach and prevent repetition.

The Lead Investigator will prepare an **incident report** setting out (where applicable):

- a summary of the security breach;
- the people involved in the security breach
- details of the information, IT systems, equipment or devices involved in the security breach and any information lost or compromised as a result of the incident;
- how the breach occurred;
- actions taken to resolve the breach;
- impact of the security breach;
- unrealised, potential consequences of the security breach;
- possible courses of action to prevent a repetition of the security breach;
- side effects, if any, of those courses of action; and
- recommendations for future actions and improvements in data protection as relevant to the incident.

This report will be presented to the full parish council.

Step 4: Notification

On the basis of the evaluation of risks and consequences, the Lead Investigator will determine whether it is necessary to notify the breach to others outside Dalton Parish Council. For example:

- the Police
- individuals (data subjects) affected by the breach
- the Information Commissioner's Office
- the press/media
- the Parish Councils insurers
- bank or credit card companies
- external legal advisers

As well as deciding **who** to notify, the Lead Investigator must consider:

- **What** is the message that needs to be put across?

In each case, the notification should include as a minimum:

- a description of how and when the breach occurred;
- what data was involved; and
- what action has been taken to respond to the risks posed by the breach.

When notifying individuals, the Lead Investigator should give specific and clear advice on what steps they can take to protect themselves, what the Parish Council is willing to do to assist them and should provide details of how they can contact the Parish Council for further information.

- **How to communicate the message?**
  What is the most appropriate method of notification (e.g. are there large numbers of people involved? Does the breach involve sensitive data? Is it necessary to write to each individual affected? Is it necessary to seek legal advice on the wording of the communication?).

- **Why are we notifying?**
  Notification should have a clear purpose, e.g. to enable individuals who may have been affected to take steps to protect themselves (e.g. by cancelling a credit card or changing a password), to allow regulatory bodies to perform their functions, provide advice and deal with complaints, etc.

Guidance is available on the ICO website under Data Protection principle 7 Data Security.

Step 5: Evaluation and Response

Subsequent to a data security breach, the Lead Investigator with any relevant stakeholders in the Parish Council will conduct a review to ensure that the steps taken during the incident were appropriate and to identify areas that may need to be improved.

The Lead Investigator will send a copy of all data security breach reports to the full Parish Council.

Considerations are:-

- What action needs to be taken to reduce the risk of future breaches and minimise their impact?
- Whether policies procedures or reporting lines need to be improved to increase the effectiveness of the response to the breach?
- If there are any weak points in security controls that need to be strengthened?
- If staff and users of services are aware of their responsibilities for information security and adequately trained?
- If additional investment is required to reduce exposure and if so what are the resource implications?

APPENDIX 1 –DATA SECURITY BREACH REPORT FORM

Please act promptly to report any data security breaches. If you discover a data security breach, please notify the Chair of the Parish Council and Clerk.

Section 1: Notification of Data Security Breach	To be completed by person reporting incident
Date incident was discovered:	
Date(s) of incident:	
Place of incident:	
Name of person reporting incident:	
Contact details of person reporting incident (email address, telephone number):	
Brief description of incident or details of the information lost:	
Number of Data Subjects affected, if known:	
Has any personal data been placed at risk? If, so please provide details:	
Brief description of any action taken at the time of discovery:	
For Dalton Parish Council use	
Received by:	
On (date):	
Forwarded for action to:	
On (date):	

Section 2: Assessment of Severity	To be completed by Lead Investigator
Details of the IT systems, equipment, devices, records involved in the security breach:	
Details of information loss:	
What is the nature of the information lost?	
How much data has been lost? If laptop lost/stolen: how recently was the laptop backed up?	
Is the information unique? Will its loss have adverse operational, research, financial legal, liability or reputational consequences for the Parish Council or third parties?	
How many data subjects are affected?	
Is the data bound by any contractual security arrangements?	
What is the nature of the sensitivity of the data? Please provide details of any types of information that fall into any of the following categories:	
HIGH RISK personal data o **Sensitive personal data** (as defined in the Data Protection Act) relating to a living, identifiable individual's a) racial or ethnic origin; b) political opinions or religious or philosophical beliefs; c) membership of a trade union; d) physical or mental health or condition or sexual life; e) commission or alleged commission of any offence, or f) proceedings for an offence committed or alleged to have been committed by the data subject, the disposal of such proceedings or the sentence of any court in such proceedings.	
o Information that could be used to commit identity fraud such as personal bank account and other financial information and national identifiers, such as National Insurance Number and copies of passports and visas;	
o Personal information relating to vulnerable adults and children;	
o Detailed profiles of individuals including information about work performance, salaries or personal life that would cause significant damage or distress to that person if disclosed;	

o Security information that would compromise the safety of individuals if disclosed.	
Category of incident (0-6):	
Reported to all Parish Councillors on:	

Section 3: Action taken	
Incident number	**e.g. /year/001**
Report received by:	
On (date):	
Action taken by responsible officer/s:	
Was incident reported to Police?	**Yes/No** **If YES, notified on (date):**
Follow up action required/recommended:	
Reported to Parish Council (date):	
Reported to other internal stakeholders (details, dates):	
For use of Parish Council	
Notification to ICO	**YES/NO If YES, notified on:** **Details:**
Notification to data subjects	**YES/NO If YES, notified on:** **Details:**
Notification to other external, regulator/stakeholder	**YES/NO If YES, notified on:** **Details:**