
Jane Austin
*Executive Officer*

Moulton Parish Council
Moulton Community Centre - Sandy Hill
Reedings, Moulton, Northants, NN3 7AX
**t: 01604 642202**
**e:** info@moultonparishcouncil.org.uk
**w:** www.moultonnorthants-pc.gov.uk

# Data Breach Policy

## 1. Purpose and Scope

Moulton Parish Council is committed to keeping data secure and as such this document is an integral part of demonstrating Data Protection Act 2018/UK GDPR compliance to ensure personal data breaches are addressed properly, appropriately and in a timely manner.

Northamptonshire County Association of Local Councils (NCALC) Currently acts as the Data Protection Officer (DPO) on behalf of Moulton Parish Council.

## 2. Legal Responsibility & Policy Support

Data Protection Act 2018
UK General Data Protection Regulation

## 3. What is a Personal Data Breach?

The UK Information Commissioner's Office (ICO) defines a personal data breach as:

"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.

Examples include but are not limited to:

- 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.

Moulton Parish Council takes the security of personal data seriously, computers are password protected and hard copy files are kept in locked cabinets. However, if a breach occurs.

There are three breach notification obligations:

1. Data processor to notify data controller.
2. Data controller to notify their Supervisory Authority (for the UK this is the ICO).
3. Data controller to notify the data subject.

## 4. Consequences of a Data Breach

A breach of personal data may result in a loss of control of personal data, discrimination, identity theft or fraud, financial loss, damage to reputation, loss of confidentiality of personal

data, damage to property or social disadvantage. Therefore, a breach, depending on the circumstances of the breach, can have a range of effects on individuals.

## 5. Reporting a Breach

Any Councillor or Officer (or data processor) who becomes aware of a breach must report it immediately to the Executive Officer.

If the breach occurs or is discovered outside normal working hours, it must be reported as soon as is possible.

The Executive Officer will complete will enter the details into the Personal Data Breach Form and inform the DPO.

## 6. Incident investigation, Containment and Recovery

The DPO will firstly determine if the breach is still occurring. If so, the appropriate steps will be taken immediately to minimise the effect of the breach.

An initial assessment will be made by the DPO in liaison with Executive Officer to establish the severity of the breach.

The DPO and Executive Officer will:

Investigate the breach and assess the risks associated with it, for example, the potential adverse consequences for individuals, how serious or substantial those are and how likely they are to occur. The investigation will need to take into account the following:

The type of data involved.

- Its sensitivity.
- The protections that are in place (e.g., encryptions).
- What has happened to the data (e.g., has it been lost or stolen).
- Whether the data could be put to any illegal or inappropriate use.
- Data subject(s) affected by the breach, number of individuals involved and the potential effects on those data subject(s).
- Whether there are wider consequences to the breach.
- If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms.
- Establish whether there is anything that can be done to recover the personal data and limit the damage the breach could cause.
- Establish who may need to be notified as part of the initial containment.
- Determine the suitable course of action to be taken to ensure a resolution to the incident.

A record will be kept of any personal data breach, regardless of whether notification was required.

## 7. Reporting the incident to the ICO

The DPO will establish whether the Information Commissioner's Office will need to be notified of the breach, and if so, notify them without undue delay and, where feasible, not later than 72 hours after having become aware of the breach of when the breach was first detected. If the ICO is not informed within 72 hours, Moulton Parish Council via the DPO must give reasons for the delay when they report the breach.

Every incident will be assessed on a case-by-case basis. However, the ICO must be notified if the breach:

- Is likely to result in a risk to the rights and freedoms of the individuals.

- Will result in a risk of damage to reputation, financial implications, confidentially loss, and discrimination, social and economic disadvantages that may occur to the concerned individual.

The following information must be provided to the ICO:

- The categories and approximate number of individuals concerned.
- The categories and approximate number of personal data records concerned.
- The name and details of the DPO.
- A description of the likely consequences of the personal data breach.
- A description of the measures taken, or proposed to be taken, to deal with the personal data breach and where appropriate of the measures taken to mitigate any possible adverse effects.

Breaches can be reported to the ICO via their website. https://ico.org.uk/for-organisations/report-a-breach/

## 8. Notifying the affected individuals

Individuals whose personal data has been affected by the incident, and where it has been considered likely to result in a high risk of adversely affecting that individual's rights and freedoms, will be informed without undue delay.

Notification will include:

- A description of how and when the breach occurred, and the data involved.
- Specific and clear advice will be given on what the individual(s) can do to protect themselves.
- What action has already been taken to mitigate the risks.
- The contact details of the DPO.

Moulton Parish Council will not need to communicate with an individual if the following applies:

- It has implemented appropriate technical and organisational measures (i.e. Encryption) so those measures have rendered the personal data unintelligible to any person not authorised to access it.
- It has taken subsequent measures to ensure that the high risk to rights and freedoms of individuals is no longer likely to materialise, or
- It would involve a disproportionate effort.

However, the ICO must still be informed even if the above measures are in place.

## 9. Evaluation and response

Once the incident has been contained, the DPO will carry out a full review of the causes of the breach; the effectiveness of the response(s) and whether any changes to systems, policies and procedures should be undertaken.

Existing controls will be reviewed to determine their adequacy, and whether any corrective action should be taken to minimise the risk of similar incidents occurring.

The review will consider:

- Where and how personal data is held and where and how it is stored.
- Where the biggest risks lie including identifying potential weak points within existing security measures.
- Whether methods of transmission are secure, sharing minimum amount of data

necessary.
- Staff awareness.
- Implementing a data breach plan and identifying a group of individuals responsible for reacting to reported breaches of security.

The breach response procedure will be revised and reissued it if necessary.

## 10. Data Processers Duty to Inform Moulton Parish Council

If a data processor (i.e. payroll provider) becomes aware of a personal data breach, it must notify Moulton Parish Council without undue delay. It is then Moulton Parish Council's responsibility to inform the DPO and/or the ICO, it is not the data processors responsibility to notify the DPO or ICO.

## 11. Records of Data Breaches

All data breaches must be recorded whether they are reported to individuals. This record will help to identify system failures and should be used to improve the security of personal data.

| Date of breach | Type of breach | Number of individuals affected | Date reported to ICO/individual | Actions to prevent breach recurring |
|---|---|---|---|---|
| | | | | |
| | | | | |
| | | | | |
| | | | | |

## 12. Annex: Article 33

Notification of a personal data breach to the supervisory authority.

12.1 In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.

12.2 The processor shall notify the controller without undue delay after becoming aware of a personal data breach.

12.3 The notification referred to in paragraph 1 shall at least:

- Describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned, and the categories and approximate number of personal data records concerned.
- Communicate the name and contact details of the data protection officer or other contact point where more information can be obtained.
- Describe the likely consequences of the personal data breach.
- 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.

12.4 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.

12.5 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 33.

## 13. Annex: Article 34

Communication of a personal data breach to the data subject.

13.1 When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay.

13.2 The communication to the data subject referred to in paragraph 1 of this Article shall describe in clear and plain language the nature of the personal data breach and contain at least the information and measures referred to in points (b), (c) and (d) of Article 33(3).

13.3 The communication to the data subject referred to in paragraph 1 shall not be required if any of the following conditions are met:

- The controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, particularly those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption.
- The controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects referred to in paragraph 1 is no longer likely to materialise.
- It would involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.

13.4 If the controller has not already communicated the personal data breach to the data subject, the supervisory authority, having considered the likelihood of the personal data breach resulting in a high risk, may require it to do so or may decide that any of the conditions referred to in paragraph 3 are met.

**This policy is reviewed annually by the Executive Officer and submitted to the full council for approval.**

**Last Reviewed:** **January 2024**
**Review Due:** **January 2025**