Funtington

Parish Council

Data Breach Policy

Version	1
Name of ratifying body	Funtington Parish Council
Date ratified	July 2021
Policy owner	Clerk: Funtington Parish Council
Date issued	July 2021
Review date	June 2023 (unless requirements change)
Electronic location	Funtington Parish Website www.funtingtonpc.org
In the case of hard copies of this policy the content can only be assured to be accurate on the date of issue marked on the document. For assurance that the most up to date policy is being used, staff should refer to the version held on the Funtington website www.funtingtonpc.org	

1. INTRODUCTION

The General Data Protection Regulations (GDPR) defines a personal data breach as

"a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed".

Examples 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
- Loss of availability of personal data

Funtington Parish Council takes the security of personal data seriously: Council computers are password protected and hard copy files are securely stored.

2. Consequences of a personal 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.

3. Funtington Parish Council's duty to report a breach

Advice from the Information Commissioner's Office (ICO) is that not every breach is reportable to the ICO, but every breach is recordable internally. The flowchart appended to this document is taken from the guidelines produced by the Article 29 Data Protection Working Party and was adopted in February 2018. All data controllers should use this flowchart to determine the severity of the breach which will determine if the breach is reportable to the ICO.

If the data breach is likely to result in a risk to the rights and freedoms of the individual, the breach must be reported to the individual and ICO without undue delay and, where feasible, not later than 72 hours after having become aware of the breach. The Data Protection Officer (DPO - the Clerk) must be informed immediately so they are able to report the breach to the ICO within the 72 hour time-frame.

If the ICO is not informed within 72 hours, Funtington Parish Council, via the DPO, must give reasons for the delay when they report the breach.

If there is any doubt about whether or not the breach is reportable, the Clerk will contact the ICO on 0303 123 1113

When notifying the ICO of a breach, Funtington Parish Council must:

a. Describe the nature of the breach including the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned

b. Communicate the name and contact details of the DPO

c. Describe the likely consequences of the breach

d. Describe the measures taken or proposed to be taken to address the personal data breach including, measures to mitigate its possible adverse effects.

When notifying the individual affected by the breach, Funtington Parish Council must provide the individual with (b)-(d) above.

Funtington Parish Council would 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 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.

4. Data processors duty to inform Funtington Parish Council

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

5. Records of data breaches

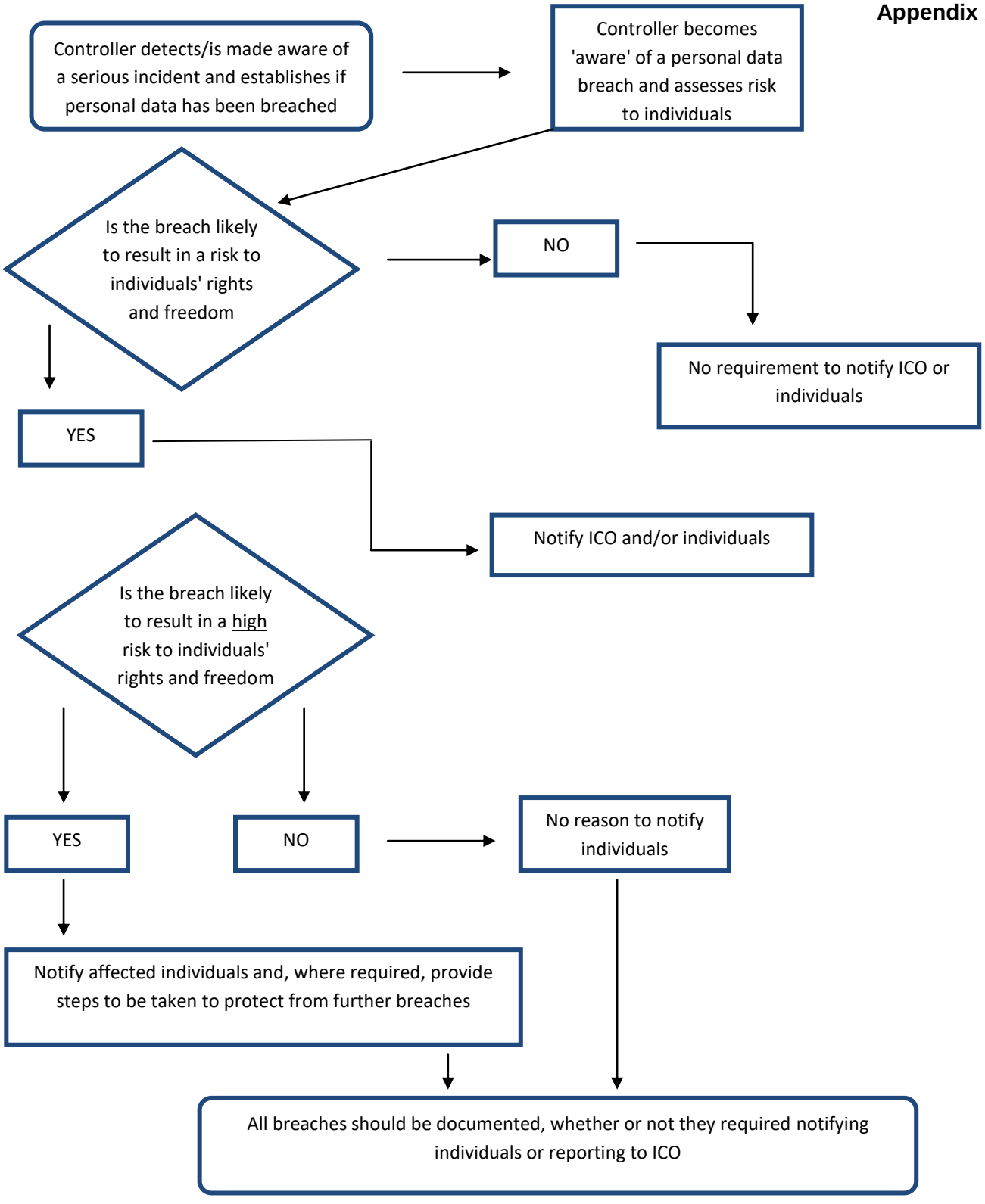
All data breaches must be recorded whether or not they are reported to individuals. This record will help to identify system failures and should be used as a way to improve the security of personal data.

Date of Breach	Type of Breach	Number of Individuals affected	Date reported to ICO	Actions to prevent a recurrence

To report a data breach

Use the ICO online system: https://ico.org.uk/for-organisations/report-a-breach

Appendix A


Controller detects/is made aware of a serious incident and establishes if personal data has been breached
Controller becomes 'aware' of a personal data breach and assesses risk to individuals
Is the breach likely to result in a risk to individuals' rights and freedom
NO
No requirement to notify ICO or individuals
YES
Notify ICO and/or individuals
Is the breach likely to result in a high risk to individuals' rights and freedom
YES
NO
No reason to notify individuals
Notify affected individuals and, where required, provide steps to be taken to protect from further breaches
All breaches should be documented, whether or not they required notifying individuals or reporting to ICO