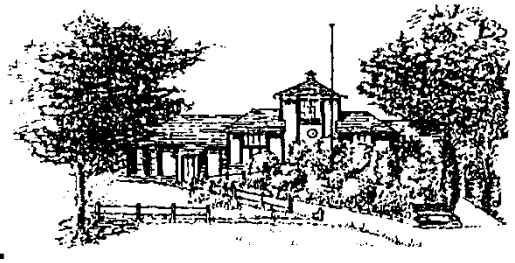

MOBBERLEY PARISH COUNCIL

Data Breach Policy

Last Review June 2023. Next Review June 2025

The Data Protection Act 2019 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

Mobberley Parish Council takes the security of personal data seriously, computers are password protected and hard copy files are kept in locked cabinets.

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.

Mobberley 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.

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.

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

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

i. 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

ii. Describe the likely consequences of the breach

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

Mobberley 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 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.

Data processors duty to inform Mobberley Parish Council

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

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.

Record of Data Breaches

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

To report a data breach, use the ICO online system: https://ico.org.uk/for-organisations/report-a-breach/

SUBJECT ACCESS REQUEST (SAR)

1. UPON RECEIPT OF A SAR, MOBBERLEY PARISH COUNCIL (TPC) WILL:

(a) Verify whether MPC is the controller of the data subject's personal data. If it is not a controller, but merely a processor, MPC will inform the data subject and refer them to the actual controller.

(b) Verify the identity of the data subject; if needed, request any further evidence on the identity of the data subject.

(c) Verity the access request; is it sufficiently substantiated? Is it clear to the data controller what personal data is requested? If not: request additional information.

(d) Verify whether requests are unfounded or excessive (in particular because of their repetitive character); if so, MPC may refuse to act on the request or charge a reasonable fee.

(e) Promptly acknowledge receipt of the SAR and inform the data subject of any costs involved in the processing of the SAR.

(f) Verify whether MPC processes the data requested. If it does not process any data, inform the data subject accordingly. At all times make sure the internal SAR procedure is followed and progress can be monitored.

(g) Ensure data will not be changed as a result of the SAR. Routine changes as part of the processing activities concerned are permitted.

(h) Verify whether the data requested also involves data on other data subjects and make sure this data is filtered before the requested data is supplied to the data subject; if data cannot be filtered, ensure that other data subjects have consented to the supply of their data as part of the SAR.

2. RESPONDING TO A SAR

(a) Mobberley Parish Council will respond to a SAR within one month after receipt of the request:

(i) If more time is needed to respond to complex requests, an extension of another two months is permissible, provided this is communicated to the data subject in a timely manner within the first month;

(ii) If the council cannot provide the information requested, it should inform the data subject on this decision without delay and at the latest within one month of receipt of the request.

(b) If a SAR is submitted in electronic form, any personal data should preferably be provided by electronic means as well.

(c) If data on the data subject is processed, make sure to include as a minimum the following information in the SAR response:

(i) the purposes of the processing;

(ii) the categories of personal data concerned;

(iii)the recipients or categories of recipients to whom personal data has been or will be disclosed, in particular in third countries or international organisations, including any appropriate safeguards for transfer of data, such as Binding Corporate Rules or EU model clauses ;

(iv)where possible, the envisaged period for which personal data will be stored or, if not possible, the criteria used to determine that period;

(v) the existence of the right to request rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;

(vi) the right to lodge a complaint with the Information Commissioners Office ("ICO");

(vii) if the data has not been collected from the data subject: the source of such data;

(viii)the existence of any automated decision-making, including profiling and any meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

(d) Mobberley Parish Council will provide a copy of the personal data undergoing processing.

ADOPTED BY MOBBERLEY PARISH COUNCIL (SIGNED BY CHAIR)

…….

DATE…….