# General Data Protection Regulation (GDPR)

## Data Protection Principles

## Information That We Will Publish or Disclose

## Information for the Information Commissioner's Office (ICO)

## The Role of Data Protection Officers

---

### DATA PROTECTION PRINCIPLES

Schedule 1 to the Data Protection Act lists the data protection principles in the following terms:

1. Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless
   (a) at least one of the conditions in Schedule 2 is met, and
   (b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.

2. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

4. Personal data shall be accurate and, where necessary, kept up to date.

5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

6. Personal data shall be processed in accordance with the rights of data subjects under this Act.

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

8. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

---

### INFORMATION THAT WE WILL PUBLISH OR DISCLOSE

**Organisation type**

Public body

**Organisation name**

Marham Parish Council

**Organisation address**

The Old School House, High Street, Stoke Ferry, King's Lynn, Norfolk, PE33 9SF, UNITED KINGDOM

**Customer enquiries contact details**

Sara Porter, Parish Clerk, The Old School House, High Street, Stoke Ferry, King's Lynn, Norfolk, PE33 9SF, UNITED KINGDOM, parishclerk.marhampc@gmail.com

**Sector**

Local Government

**Nature of work**

Parish & Community Council

**Are you a public authority?**

Yes

**Is your organisation a charity or have exempt charitable status?**

No

**Does your organisation have more than 249 staff?**

No

**Details about the information you process**

Nature of work - Provision of council services

**Description of processing**

The following is a broad description of the way this organisation/data controller processes personal information. To understand how your own personal information is processed you may need to refer to any personal communications you have received, check any privacy notices the organisation has provided or contact the organisation to ask about your personal circumstances.

**Reasons/purposes for processing information**

We process personal information to enable us to carry out our statutory duties. We also process personal information to promote our services; undertake fundraising; maintain our accounts and records; manage and support our employees.

**Type/classes of information processed**

We process information relevant to the above reasons/purposes. This may include:

- personal details
- family details
- lifestyle and social circumstances
- education and employment details
- financial details
- goods and services

We also process sensitive classes of information that may include: physical or mental health details; racial or ethnic origin.

**Who the information is processed about**

We process personal information about:

- employees

- suppliers
- complainants, enquirers
- business contacts
- professional advisers and consultants
- residents of the parish
- elected representatives and holders of public office
- members of the parish council

**Who the information may be shared with**

We sometimes need to share the personal information we process with the individual themself and also with other organisations. Where this is necessary we are required to comply with all aspects of the Data Protection Act (DPA). What follows is a description of the types of organisations we may need to share some of the personal information we process with for one or more reasons.

**Where necessary or required we share information with:**

- educators and examining bodies
- suppliers and service providers
- persons making an enquiry or complaint
- local government
- press and the media
- family, associates and representatives of the person whose personal data we are processing
- current, past and prospective employers
- financial organisations

**Additional reasons**

**Transferring information overseas**

**Do you transfer data outside the European Economic Area (EEA)?**

No

**Does this cover all your processing of personal information?**

Yes

---

## INFORMATION FOR THE INFORMATION COMMISSIONER'S OFFICE (ICO)

**Main contact details**

Sara Porter, Parish Clerk, The Old School House, High Street, Stoke Ferry, King's Lynn, Norfolk, PE33 9SF, UNITED KINGDOM, parishclerk.marhampc@gmail.com

**Person completing the registration**

Mrs Sara Porter, Parish Clerk

**Someone in my place of work is responsible for making sure we comply with the Data Protection Act**

Yes

**Relevant people in my place of work have been trained in how to handle personal information**

Yes

**When collecting personal information, we tell people how we will use it**

Yes

**We have a process in place so we can respond to requests for the personal information we hold**

Yes

**We keep records of people's personal information up to date and don't keep it longer than necessary**

Yes

**We have measures in place to keep the personal data we hold safe and secure**

Yes

**Declaration by Parish Clerk**

☑ I declare that, to the best of my knowledge and belief, the details I have given in the registration are correct. I confirm that I am authorised to act on behalf of the organisation (data controller) named in this registration. I am aware that if I have provided false information, this may be an offence.

---

## THE ROLE OF DATA PROTECTION OFFICERS

### 1. What Does a Data Protection Officer Do?

(a) The GDPR sets out in detail the minimum responsibilities of the Data Protection Officer ('DPO') role. GDPR specifies that DPOs 'should assist the controller or the processor to monitor internal compliance with this Regulation'.

(b) A DPO's duties include:

(i) informing and advising the Council and its staff of their obligations in the GDPR and other data protection laws;

(ii) monitoring compliance of the Council, both its practices and policies, with the GDPR and other data protection laws;

(iii) raising awareness of data protection law; providing relevant training to staff and Councillors;

(iv) carrying out data protection-related audits;

(v) providing advice to the Council, where requested, in relation to the carrying out of data protection impact assessments ('DPIAs') and the Council's wider obligations with regard to DPIAs; and

(vi) acting as a contact point for the Information Commissioner's Office.

(c) As part of these duties to monitor compliance, DPOs may, in particular:

(i) collect information to identify processing activities;

(ii) analyse and check the compliance of processing activities; and

(iii) inform, advise and issue recommendations to the controller or the processor

(d) Monitoring of compliance does not mean that it is the DPO is personally responsible where there is an instance of non-compliance. The GDPR makes it clear that it is the controller, not the DPO, who is

required to 'implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation.'

(e) The appointed DPO must at all times have regard to 'the risk associated with the processing operations, taking into account the nature, scope, context and purposes of processing.' This is an overarching obligation which means that the role of the DPO will vary in proportion to the risks to the rights of individuals affected by the Council's processing of personal data.

(f) The DPO should 'cooperate with the supervisory authority'(in the UK, this is the Information Commissioners Office ('ICO') and 'act as a contact point for the supervisory authority on issues relating to processing, and to consult, where appropriate, with regard to any other matter'.

(g) It is the controller or the processor, not the DPO, who is required to 'maintain a record of processing operations under its responsibility' or 'maintain a record of all categories of processing activities carried out on behalf of a controller'.

## 2. DPOs and DPIAs

(a) A data controller (and not the DPO) is required to carry out a data protection impact assessment ('DPIA') under the GDPR in certain circumstances.

(b) The controller must 'seek advice' from the DPO when carrying out a DPIA. DPOs have the duty to 'provide advice where requested as regards the DPIA and monitor its performance'.

(c) It is recommended that controllers should seek the advice of the DPO on the following issues:

(i) Whether or not to carry out a DPIA;

(ii) What methodology to follow when carrying out a DPIA;

(iii) Whether to carry out the DPIA in-house or whether to outsource what it safeguards (including technical and organisational measures) to apply to mitigate any risks to the rights and interests of the data subjects; and

(iv) Whether or not the data protection impact assessment has been correctly carried out and whether its conclusions (whether or not to go ahead with the processing and what safeguards to apply) are in compliance with the GDPR.

(d) If the controller disagrees with the advice provided by the DPO, the DPIA documentation should specifically justify in writing why the advice has not been taken into account.

## 3. Data Controllers and Processors Should Ensure That:

(a) The DPO is invited to participate regularly in meetings of senior and middle management. For Councils, this would include meetings of full Council and relevant committee meetings.

(b) The DPO's name and contact details are provided to ICO;

(c) The DPO should be available to advise/ support Councillors and relevant staff on data protection issues;

(d) The DPO is present when decisions with data protection implications are taken;

(e) All relevant information must be passed on to the DPO in a timely manner in order to allow him or her to provide adequate advice;

(f) The opinion of the DPO must always be given due weight. In case of disagreement it is good practice to document the reasons for not following the DPO's advice;

(g) The DPO should be promptly consulted once a data breach or another incident has occurred. This is good practice since the DPO will often have been involved in implementing data protection polices such as breach reporting and it will be important for the DPO to assess whether the policies work operationally.

## 4. Personal Data Breaches

A data breach is a breach of security leading to 'accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data'. The GDPR introduces a duty to report certain types of data breaches to the ICO and in some cases to the individuals concerned.

The Council must demonstrate that it has appropriate security, technical and organisational measures in place to protect against a breach. If there is no risk of harm to an individual (for example because some low risk data has been inadvertently released or made public such as an email address) then this type of breach would not need to be reported. Unauthorised access to data that could be used to steal someone's identity such as their banking data must be reported.

- The DPO should be involved after the Council becomes aware of a data breach.
- Councillors, staff, contractors and the Council's data processors should be briefed on personal data breach avoidance, and on what to do in the event that a breach occurs.
- Examples of personal data breaches and steps to avoid them include:
  - Emails and attachments being sent to the wrong person, or several people – it is easy to click the wrong recipient. Slow down, check thoroughly before clicking 'send'.
  - The wrong people being copied into emails and attachments. Use BCC (Blind Carbon Copy) where necessary.
  - Lost memory sticks which contain unencrypted personal data – the Council should put protocols in place for memory stick usage.
  - Malware (IT) attach – ensure up to date anti-virus software is in place.
  - Equipment theft – check security provisions.
  - Loss of personal data which is unencrypted.

## 5. Parish Council's Role Checklist

| | |
|---|---|
| ☑ | Raising data protection awareness within the Council, and advising on GDPR compliance; |
| ☑ | Ensuring the implementation of the appropriate documentation to demonstrate GDPR compliance; |
| ☑ | Monitoring the implementation and compliance with policies, procedures and GDPR in general; |
| ☑ | Involvement in Council's handling of data breaches, including assisting and advising the Council with its notification to the ICO and data subjects where necessary (but it is the Council which has the obligation to notify in certain circumstances not the DPO); |
| ☑ | Liaising with the ICO, the relevant Councillors and staff and with the data subjects; |
| ☑ | Monitoring Data Protection Impact Assessments; |
| ☑ | Cooperating with and acting as the contact point for the ICO on issues relating to processing |