

# Marchwood Parish Council

Marchwood Village Hall  
Village Centre  
Marchwood  
SO40 4SX

Telephone: 023 8086 0273

Email: [office@marchwoodparishcouncil.org.uk](mailto:office@marchwoodparishcouncil.org.uk)



6<sup>th</sup> October 2020.

Dear Councillor, a meeting of the Parish Council will be held via a scheduled video meeting Monday 12<sup>th</sup> October 2020 at 7.30pm. It will be conducted using the Zoom video conferencing solution.

Members of the public should contact the Clerk to the Council for details on how to connect to the meeting.

*Brendan V. Gibbs*

Clerk to the Council

## AGENDA

1. **Apologies for absence.**
2. **Declarations of Interest.**
3. **Solent Gateway Ltd. To receive a presentation on their “Options for the future” Consultation.**
4. **Public participation – Should not exceed 15 minutes in duration. Standing Order 3 (e) & (f) December 2019.**
5. **The Chairman’s report.**
6. **Minutes: To confirm the minutes of the meeting held on the 27th July 2020.**
7. **Reports from the New Forest District Councillors.**
8. **Report from the Hampshire County Councillor.**
9. **Policies to be reviewed – Report A.**

**Data Protection Policy.**

**FOI Vexatious or Repeated Requests Policy.**

10. **Co-option process.**
  - a) **Applications have been received from Mrs Alice Ushamba and Mr Rory Collis with reference to the current vacancies on the Parish Council.**
  - b) **To consider these applications.**
11. **Committee minutes to be received as follows:**

**Planning: 6<sup>th</sup> July 2020, 3<sup>rd</sup> August 2020, 7<sup>th</sup> September 2020.**  
**Policy & Resources: 15<sup>th</sup> June 2020.**  
**Amenities: 10<sup>th</sup> February 2020.**

- 12. Exempt Business: To pass a resolution in accordance with the Public Bodies (Admission to Meetings) Act 1960 to exclude the public and press from the discussion of the following matters where publicity might be prejudicial to the special nature of the business.**

Two personnel issues affecting all employees.

Other personnel issues.

**Members of the Press and Public are welcome to attend any meeting of the Parish Council. These rights are enshrined in the Public Bodies (Admission to Meetings) Act 1960 and the Openness of Local Government Bodies Regulations 2014.**

**All in attendance should be aware that filming, photographing, recording, broadcasting or transmitting the proceedings of the Council may occur during the meeting.**

**Policy Review 2020-21**

Dear Councillors,

At Monday's meeting there are a further two policy documents to confirm.

These policies were reviewed by the Policy & Resources Committee back in June 2020 and were found to be in order.

Data Protection Policy

Freedom of Information Act 2000 Vexatious or Repeated Requests Policy.

As was mentioned at the P&R Meeting in June there was a lot of work was done on a Data Protection Policy in 2018 but it would appear that the policy was never formally approved at that time.

I am now re-issuing a slightly updated and re-formatted version for further consideration by the committee.

I am also proposing a policy to better manage requests for information under the Freedom of Information Act 2000.

Currently, we have no policy to deal with vexatious or repeated requests for information.

I would like to stress there are no issues with this topic at the moment but it would seem prudent that the Parish Council has a policy in place rather than have to refer to the Information Commissioner's Office for help and advice at a future date.

Brendan.



**Marchwood Parish Council**  
**Data protection policy (GDPR compliant)**

**1. Aim and scope of policy**

This policy applies to the processing of personal data in manual and electronic records kept by the Parish Council in connection with its human resources function as described below. It also covers the Parish Council's response to any data breach and other rights under the General Data Protection Regulation.

This policy applies to the personal data of job applicants, existing and former employees, apprentices, volunteers, placement students, workers and self-employed contractors. These are referred to in this policy as relevant individuals.

- "Personal data" is information that relates to an identifiable person who can be directly or indirectly identified from that information, for example, a person's name, identification number, location, online identifier. It can also include pseudonymised data.
- "Special categories of personal data" is data which relates to an individual's health, sex life, sexual orientation, race, ethnic origin, political opinion, religion, and trade union membership. It also includes genetic and biometric data (where used for ID purposes).
- "Criminal offence data" is data which relates to an individual's criminal convictions and offences. "Data processing" is any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

The Parish Council makes a commitment to ensuring that personal data, including special categories of personal data and criminal offence data (where appropriate) is processed in line with GDPR and domestic laws and all its employees conduct themselves in line with this, and other related, policies. Where third parties process data on behalf of the Parish Council, the Parish Council will ensure that the third party takes such measures in order to maintain the Parish Council's commitment to



## **Marchwood Parish Council**

### **Policy for dealing with vexatious or repeated requests for information.**

The Freedom of Information Act 2000 (FOIA) gives the public a right of access to information held by public authorities.

#### **1. Aim and scope of policy**

Marchwood Parish Council (the Council) is committed to dealing with genuine enquiries and requests for information appropriately and in accordance with our other policies. Whilst the Council aims to be open and transparent, it is aware of the need to ensure that its time is not taken up pursuing vexatious or repeated requests and that staff and councillors are protected from such enquiries.

The Council also has a responsibility to ensure the effective use of its resources, which are funded by the council tax payers of the parish of Marchwood

Our policy is to follow the latest guidance from the Information Commissioners Office as follows to ensure that requests that are deemed to be repeated or vexatious are dealt with fairly.

#### **2. Dealing with vexatious requests – Section 14 (1) Freedom of Information Act:**

Under section 14(1) of the Act, public authorities do not have to comply with vexatious requests.

Section 14(1) may be used in a variety of circumstances where a request, or its impact on a public authority, cannot be justified.

Whilst public authorities should think carefully before refusing a request as vexatious they should not regard section 14(1) as something which is only to be applied in the most extreme of circumstances.

- Section 14(1) can only be applied to the request itself and not the individual who submitted it.
- Sometimes a request may be so patently unreasonable or objectionable that it will obviously be vexatious.

- In cases where the issue is not clear-cut, the key question to ask is whether the request is likely to cause a disproportionate or unjustified level of disruption, irritation or distress.
- This will usually be a matter of objectively judging the evidence of the impact on the authority and weighing this against any evidence about the purpose and value of the request.
- The public authority may also take into account the context and history of the request, where this is relevant.
- Although not appropriate in every case, it may be worth considering whether a more conciliatory approach could help before refusing a request as vexatious.
- A public authority must still issue a refusal notice unless it has already given the same individual a refusal notice for a previous vexatious request, and it would be unreasonable to issue another one.
- If the cost of compliance is the only or main issue, we recommend that the authority should consider first whether section 12 applies (there is no obligation to comply where the cost of finding and retrieving the information exceeds the appropriate limit).

### **3. Dealing with repeat requests – Section 14 (2) Freedom of Information Act:**

Under Section 14(2) of the Act, a public authority does not have to comply with a request which is identical, or substantially similar to a previous request submitted by the same individual, unless a reasonable period has elapsed between those requests.

- A public authority may only apply Section 14(2) where it has either;
- previously provided the same requester with the information in response to an earlier FOIA request; or
- previously confirmed the information is not held in response to an earlier FOIA request from the same requester.
- If neither of these conditions applies then the public authority must deal with the request in the normal manner.
- A request will be identical if both its scope and its wording precisely matches that of a previous request.
- It will be substantially similar if;
- The wording is different but the scope of the request is the same; or
- The scope does not differ significantly from that of the previous request.



The reasonable interval is largely dependent upon the likelihood of any of the information caught within the scope of the request differing or having changed from that previously provided.

If the information is unlikely to be different then the authority will need to consider the amount of time between requests and decide whether this is enough to make it reasonable to provide the same information again.

The Public Authority must issue a refusal notice unless it has already served the requester with a notice under Section 14(2) in response to a previous request for the same information, and it would be unreasonable to issue another one.

#### **4. Alterations and amendments to this policy**

Marchwood Parish Council reserves the right to amend or withdraw this procedure at its absolute discretion, in accordance with the needs of the Council.

#### **5. Amendment Record**

Version 1: Initial issue

protecting data. In line with GDPR, the Parish Council understands that it will be accountable for the processing, management and regulation, and storage and retention of all personal data held in the form of manual records and on computers.

## **2. Types of data held**

Personal data is kept in personnel files or within the Parish Council's HR systems. The following types of data may be held by the Parish Council, as appropriate, on relevant individuals:

- name, address, phone numbers - for individual and next of kin.
- CVs and other information gathered during recruitment.
- references from former employers.
- National Insurance numbers.
- job title, job descriptions and pay grades.
- conduct issues such as letters of concern, disciplinary proceedings.
- holiday records.
- internal performance information.
- medical or health information.
- sickness absence records.
- tax codes.
- terms and conditions of employment.
- training details.

Relevant individuals should refer to the Parish Council's privacy notice for more information on the reasons for its processing activities, the lawful bases it relies on for the processing and data retention periods.

## **3. Data protection principles**

All personal data obtained and held by the Parish Council will:

- be processed fairly, lawfully and in a transparent manner.
- be collected for specific, explicit, and legitimate purposes.
- be adequate, relevant and limited to what is necessary for the purposes of processing.
- be kept accurate and up to date. Every reasonable effort will be made to ensure that inaccurate data is rectified or erased without delay.
- not be kept for longer than is necessary for its given purpose.
- be processed in a manner that ensures appropriate security of personal data including protection against unauthorised or unlawful processing, accidental loss, destruction or damage by using appropriate technical or organisation measures.
- comply with the relevant GDPR procedures for international transferring of personal data.

In addition, personal data will be processed in recognition of an individuals' data protection rights, as follows:

- the right to be informed.
- the right of access.
- the right for any inaccuracies to be corrected (rectification).
- the right to have information deleted (erasure).
- the right to restrict the processing of the data.
- the right to portability.
- the right to object to the inclusion of any information.
- the right to regulate any automated decision-making and profiling of personal data.

#### **4. Procedures**

The Parish Council has taken the following steps to protect the personal data of relevant individuals that it holds or to which it has access and it appoints or employs employees with specific responsibilities for:

- the processing and controlling of data.
- the comprehensive reviewing and auditing of its data protection systems and procedures.
- overseeing the effectiveness and integrity of all the data that must be protected.

There are clear lines of responsibility and accountability for these different roles.

- it provides information to its employees on their data protection rights, how it uses their personal data, and how it protects it. The information includes the actions relevant individuals can take if they think that their data has been compromised in any way.
- it provides its employees with information and training to make them aware of the importance of protecting personal data, to teach them how to do this, and to understand how to treat information confidentially.
- it can account for all personal data it holds, where it comes from, who it is shared with and also who it might be shared with.
- it carries out risk assessments as part of its reviewing activities to identify any vulnerabilities in its personal data handling and processing, and to take measures to reduce the risks of mishandling and potential breaches of data

security. The procedure includes an assessment of the impact of both use and potential misuse of personal data in and by the Parish Council.

- it recognizes the importance of seeking individuals' consent for obtaining, recording, using, sharing, storing and retaining their personal data, and regularly reviews its procedures for doing so, including the audit trails that are needed and are followed for all consent decisions. The Parish Council understands that consent must be freely given, specific, informed and unambiguous. The Parish Council will seek consent on a specific and individual basis where appropriate. Full information will be given regarding the activities about which consent is sought. Relevant individuals have the absolute and unimpeded right to withdraw that consent at any time.
- it has the appropriate mechanisms for detecting, reporting and investigating suspected or actual personal data breaches, including security breaches. It is aware of its duty to report significant breaches that cause significant harm to the affected individuals to the Information Commissioner, and is aware of the possible consequences.
- It is aware of the implications international transfer of personal data internationally.

## **5. Access to data**

Relevant individuals have a right to be informed whether the Parish Council processes personal data relating to them and to access the data that the Parish Council holds about them. Requests for access to this data will be dealt with under the following summary guidelines:

- The request should be made to the Clerk at Marchwood Parish Council, The Village Hall, Marchwood, Southampton SO40 4SF.
- the Parish Council will not charge for the supply of data unless the request is manifestly unfounded, excessive or repetitive, or unless a request is made for duplicate copies to be provided to parties other than the employee making the request.
- the Parish Council will respond to a request without delay. Access to data will be provided, subject to legally permitted exemptions, within one month as a maximum. This may be extended by a further two months where requests are complex or numerous.

Relevant individuals must inform the Parish Council immediately if they believe that the data is inaccurate, either as a result of a subject access request or otherwise. The Parish Council will take immediate steps to rectify the information.

For further information on making a subject access request, employees should consult with the Clerk or Responsible Financial Officer.

## **6. Data disclosures**

The Parish Council may be required to disclose certain data/information to any person. The circumstances leading to such disclosures include:

- any employee benefits operated by third parties.
- disabled individuals - whether any reasonable adjustments are required to assist them at work.
- individuals' health data - to comply with health and safety or occupational health obligations towards the employee.
- for Statutory Sick Pay purposes.
- HR management and administration - to consider how an individual's health affects his or her ability to do their job.
- the smooth operation of any employee insurance policies or pension plans.

These kinds of disclosures will only be made when strictly necessary for the purpose.

## **7. Data security**

The Parish Council adopts procedures designed to maintain the security of data when it is stored and transported. In addition, employees must:

- ensure that all files or written information of a confidential nature are stored in a secure manner and are only accessed by people who have a need and a right to access them.
- ensure that all files or written information of a confidential nature are not left where they can be read by unauthorised people.
- check regularly on the accuracy of data being entered into computers.
- always use the passwords provided to access the computer system and not abuse them by passing them on to people who should not have them.
- use computer screen blanking to ensure that personal data is not left on screen when not in use.

Personal data relating to employees should not be kept or transported on laptops, USB sticks, or similar devices, unless authorised by the Clerk who can be contacted at Marchwood Parish Council, The Village Hall, Marchwood, Southampton SO40 4SF.

Where personal data is recorded on any such device it should be protected by:

- ensuring that data is recorded on such devices only where absolutely necessary
- using an encrypted system — a folder should be created to store the files that need extra protection and all files created or moved to this folder should be automatically encrypted
- ensuring that laptops or USB drives are not left lying around where they can be stolen.

Failure to follow the Parish Council's rules on data security may be dealt with via the Parish Council's disciplinary procedure. Appropriate sanctions include dismissal with or without notice dependent on the severity of the failure.

## **8. Breach notification**

Where a data breach is likely to result in a risk to the rights and freedoms of individuals, it will be reported to the Information Commissioner within 72 hours of the Parish Council becoming aware of it and may be reported in more than one instalment.

Individuals will be informed directly in the event that the breach is likely to result in a high risk to the rights and freedoms of that individual.

If the breach is sufficient to warrant notification to the public, the Parish Council will do so without undue delay.

## **9. Training**

New employees must read and understand the policies on data protection as part of their induction. All employees receive training covering basic information about confidentiality, data protection and the actions to take upon identifying a potential data breach.

The nominated data controller/auditors/protection officers for the Parish Council are trained appropriately in their roles under the GDPR.

All employees who need to use the computer system are trained to protect individuals' private data, to ensure data security, and to understand the consequences to them as individuals and the Parish Council of any potential lapses and breaches of the Parish Council's policies and procedures.

## **10. Records**

The Parish Council keeps records of its processing activities including the purpose for the processing and retention periods in its Data Audit Schedule.

These records will be kept up to date so that they reflect current processing activities.

## **11. Data Protection Officer**

The Parish Council's Data Protection Officer is under legislative review by the Government to exempt Parish Councils from this requirement.

## **12. Data protection compliance**

The Clerk is the Parish Council's appointed compliance officer in respect of its data protection activities. If you need any specific help or general guidance about the Council's procedures or about any specific complaint, contact the Clerk at Marchwood Parish Council, The Village Hall, Marchwood, Southampton SO40 4SF or telephone 02380 860273 or email [clerk@marchwoodparishcouncil.org.uk](mailto:clerk@marchwoodparishcouncil.org.uk)

## **13. Alterations and amendments to this policy**

Marchwood Parish Council reserves the right to amend or withdraw this procedure at its absolute discretion, in accordance with the needs of the Council.

## **14. Amendment Record**

Version 1: Initial issue