# Data Protection Policy

Fair Oak and Horton Heath

Parish Council

Adopted: September 2021
Review: March 2024

# Contents

# 1. Introduction, Purpose and Scope

## Introduction

As a Data Controller, Fair Oak and Horton Heath Parish Council (the "Council") is committed to protecting personal data processed in the performance of its duties. The Council's registration number with the Information Commissioner's Office is Z8754409. This registration is renewed annually in January each year.

To meet privacy and data protection commitments and obligations under the applicable data protection laws, the Council has implemented a privacy programme based on the data protection principles and governance obligations described in this Data Protection Policy ("Policy").

The Policy forms part of the Council's accountability framework and the Council regards the commitment to data protection as a key component of its enterprise risk management strategy and expect all Councillors, staff, volunteers and partners to apply this Policy. Infringements of this Policy will put the Council at risk of fines or enforcement action thereby limiting its ability to carry out its responsibilities and acting in the best interest of residents.

## Purpose

This Policy provides guidance on the data protection principles and related procedures, processes and controls that are required when Fair Oak and Horton Heath Parish Council processes personal data.

## Scope

This Policy applies to all those involved with the Council.

The Council expects its partners and vendors to comply with the general data protection principles, their own data protection policies, applicable legislation and aspects relating to data protection contained in contracts and agreements.

This Policy applies to both automated and manual data processing activities.

Reference in the Policy to data protection legislation means the UK Data Protection Act 2018 which incorporates the General Data Protection Regulation (GDPR 2016/679), the Privacy and Electronic Communications (EC Directive) Regulations 2003 and any legislation implemented in connection with the General Data Protection Regulation. Account has also been taken of best practice advice from the Information Commissioner's Office (ICO).

## 2. Key Definitions

**Personal Data** means any data relating to an identified or identifiable natural person. This can include (but is not limited to) names, location data, email address, photographs, IP address, account details, credit card numbers, staff records and correspondence to and from an individual.

**Special Category Data** means personal data revealing an individual's racial or ethnic origin; political opinions; religious or philosophical beliefs; trade union membership; biometric (e.g. fingerprints or facial recognition) or genetic information for the purposes of identification and information about an individual's health and sex life or sexual orientation. Information on criminal convictions or offences (including allegations) and information on children and vulnerable individuals is regarded as sensitive data.

**Processing** means any operation performed on personal data, such as collection, recording, storage, retrieval, use, combining it with other data, transmission, disclosure or deletion.

**Data Subject** means the individual to whom the personal data relates.

**Personal Data Breach** means 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.

**Data Controller** means the party which determines the purposes and means of the data processing.

**Data Processor** means the party processing personal data on behalf of a Controller, under the Controller's instructions.

**Filing System** means any structured set of personal data which is accessible according to specific criteria, whether held by automated means or manually and whether centralised, decentralised or dispersed on a functional or geographical basis.

**Council Responsibilities** include all the duties and agreed objectives of Fair Oak and Horton Heath Parish Council. It further includes the hosting of events, promoting the parish, information gathering, compliance with legal and governance obligations, enforcing policies and procedures, recording transactions, employment obligations, the handling of casework, financial and administrative tasks and other actions in the general running of the Council.

**Privacy by Design** means the Council shall implement and maintain a process such that any new processing activity, tool or functionality involved in the processing of personal data is designed and built in a way that allows it to comply with the Data Protection Principles.

**Direct Marketing** means any marketing communication to an identified individual. Blanket marketing such as leaflets, advertisements and magazine inserts are not direct marketing.

# 3. Data Categories

Fair Oak and Horton Heath Parish Council processes personal data to carry out its responsibilities and pursue Council objectives.

The personal data the Council processes includes name, surname, physical/postal address, email address, business email address, telephone number, photographs, bank account details, credit card details, CCTV footage, IP address, driver's licence, national insurance number, passport, staff records, etc.

### 3.1 Special Category and Sensitive Data

The Council currently processes only a very limited amount of personal data classified as special category data. This includes health information about staff such as sick notes and the political opinions of some Councillors through the Register of Members' Interests and Statement of Persons Nominated public declarations.

Sensitive data is occasionally processed for the purposes of Disclosure and Barring Service (DBS) checks.

The Council only holds limited data on children such as pictures from events obtained through parental consent and organised youth activities hosted by other organisations.

If in future the Council has the need to expand the processing of special category data and an exemption does not apply, explicit consent will be obtained from the individuals concerned.

The Council will ensure that the appropriate safeguarding measures are applied as required. Privacy notices will be updated to inform the individuals of how their data will be used and the processing will be reflected in the Council's Retention Schedule.

# 4. Data Protection Principles

Fair Oak and Horton Heath Parish Council complies with the following Data Protection Principles:

a) **Fairness and Transparency**: Personal data is processed fairly and individuals are informed how and why their data is processed.

b) **Lawful Processing**: Personal data, including special category and sensitive personal data, is processed lawfully with a valid legal basis.

c) **Purpose Limitation**: Personal data is only collected for a specified, explicit and legitimate purpose and any subsequent processing is only done if it is compatible with the original purpose, or consent has been obtained from the individual, or the processing is otherwise permitted by law.

d) **Data Minimisation**: Only personal data that is adequate, relevant and limited to what is necessary in relation to the purpose for the processing is collected.

e) **Data Accuracy**: The Council takes reasonable steps to ensure that personal data is accurate and kept up to date.

f) **Individual Rights**: Individuals are given the opportunity to exercise their rights as set out in Section 8 of this Policy.

g) **Storage Limitation**: Personal data is kept only for as long as it is needed for the purposes for which it was collected or for further permitted purposes. Data storage is done in compliance with the Council's Retention Policy set out in Section 7 of this Policy and the Council's Retention Schedule in Appendix 7.

h) **Data Security**: Appropriate security measures are used to protect personal data including carrying out a due diligence exercise where third parties are processing personal data on the Council's behalf.

i) **Accountability**: The Council ensures that it has appropriate policies, procedures, practices and controls in place to comply with, and are able to demonstrate compliance with, these Data Protection Principles.

In addition, taking into consideration the technology available to the Council and the cost, the Council strives to comply with the principles of Data Protection by Design and by Default.

# 5. Legal Basis for Processing

Fair Oak and Horton Heath Parish Council processes personal data according to the Lawful Processing Principle (outlined in Section 4) and ensures that at least one of the following conditions apply:

a) **Consent:** The individual has given consent for the processing of the personal data for one or more specific purposes. The individual was given enough information to understand what the consent was for and the request was presented in a clear manner that was distinguishable from other matters. The consent was given freely and was an unambiguous indication of the individual's wishes. Consent can be provided by written or oral statement but is not gained through silence, pre-ticked boxes or inactivity. When seeking consent, the Council ensures that consent is informed by always identifying the organisation and the purpose of the processing. The Council keeps a record of the consent in line with its Retention Policy and ensures that an individual can withdraw their consent at any time including when they have opted-in to receiving direct marketing communications.

b) **Performance of a Contract**: The processing is necessary for the performance of a contract to which the individual is party or in order to take steps at the request of the individual prior to entering into a contract.

c) **Legal Obligation**: The processing is necessary for compliance with a legal obligation the Council is required to meet.

d) **Vital Interests**: The processing is necessary to protect the individual or another person in order to save their life or in a serious medical situation where the person is unable to give consent.

e) **Public Interest**: The processing is necessary to perform an official public function or task that is in the public interest.

f) **Legitimate Interest**: The processing is necessary for the purposes of the legitimate interests of the Council or a third party. This does not apply where the Council's interest is overridden by the interests or fundamental rights and freedoms of the individuals especially when the data subject is a child. The Council applies purpose, necessity and balancing tests to determine if it meets the requirements for the use of this legal basis and keeps a record showing that proper consideration had been given to the interests of the individuals concerned.

Fair Oak and Horton Heath Parish Council will inform individuals of the lawful basis used through privacy notices as set out in Section 11.

# 6. Training

In keeping with the Accountability Principle and as part of the Council's accountability framework demonstrating compliance, all Council staff, Councillors and volunteers are trained on their data protection responsibilities.

Training is provided on the policies, procedures and controls in place and the general data protection principles. Individual volunteers are trained according to need or the specialist areas they support e.g. assisting at events such as the Fair Oak Carnival and Christmas events.

Training is always provided as part of an induction programme for new staff and Councillors.

Staff in positions where a high volume of personal data is processed are provided with ongoing training to keep their knowledge current and are given guidance and advice specific to their areas of responsibility.

The Council also ensures that staff and Councillors are kept up to date on new legislation and best practice through an ongoing awareness programme overseen by the Data Protection Officer.

The Council's Training Register is kept up to date by the Data Protection Officer. See Appendix 4 for the Training Register.

# 7. Data Retention Policy

Fair Oak and Horton Heath Parish Council applies the Storage Limitation Principle and ensures that data is not kept for longer than is necessary for the purpose it was collected. This applies to all staff, Councillors and volunteers.

The Council's Retention Schedule (see Appendix 7) outlines the storage periods for the personal data stored. The retention periods vary according to legal obligations and to meet the Council's business needs.

In keeping with the Accuracy Principle, the Council takes reasonable steps to review the personal data stored every two years or according to the time limits set in the Retention Schedule.

The Data Protection Officer keeps the Retention Schedule up to date and staff and Councillors are required to follow the retention periods specified. If there is a change in legislation or the specified retention periods are no longer valid, the Data Protection Officer will make the required changes to ensure ongoing compliance.

The destruction and deletion of files containing personal data take place according to the Schedule. Paper files are securely stored until they are destroyed.

Manual document destruction is performed in-house and digital document destruction is performed by deleting files from all platforms, databases, backup systems and hard drives.

Processors used by the Council are required to follow the personal data destruction arrangements outlined in agreements.

# 8. Data Subject Rights and Access Requests

Fair Oak and Horton Heath Parish Council ensures that individuals can exercise their rights as set out in legislation.

Individuals can make requests via phone, email, social media, letter or orally to a member of staff or a Councillor. The Data Protection Officer will respond on behalf of the Council.

### 8.1 Individual Rights

Data protection legislation stipulates the following rights:

**8.1.1 Right of Access:** Individuals have the right to be informed of whether personal data is held concerning them, the purpose for processing the data, the categories of data including whether the data is special category personal data, the recipients or categories of recipients that the data is shared with, the period for which the data is stored (and how that is determined) and information on the source of the data if not provided by the individual. If personal data is transferred to a third country the individual has the right to be informed of the safeguards in place. Individuals also have the right to know whether they are subject to automated decision-making such as profiling.

The Council's privacy notices make individuals aware of their rights including the right to lodge a complaint with the Information Commissioner's Office (ICO) and the right to request erasure, rectification or restriction which will also be mentioned in any response given to individuals exercising this right.

Fair Oak and Horton Heath Parish Council will provide a copy of the personal data undergoing processing free of charge. If more than one copy is requested or the request is manifestly unfounded or excessive, a reasonable fee can be charged.

**8.1.2 Right to Rectification:** Individuals have the right to have inaccurate data corrected or incomplete data completed. When a request is received exercising this right, the request needs to be sent to the Data Protection Officer as the individual responsible for ensuring the accuracy of the personal data. The individual making the request will be informed that it has been actioned on all Council records and that partners and processors have been informed to do the same.

**8.1.3 Right to Erasure:** Sometimes known as the "right to be forgotten", individuals have the right to have personal data erased in certain circumstances.

Individuals have the right to request that the Council deletes all personal data in the following circumstances:

- The personal data is no longer necessary for the purpose for which it was originally collected or processed;
- The Council is relying on consent as its lawful basis for holding the data and consent is withdrawn and there is no other legal ground for processing;
- The Council is relying on legitimate interests as its legal basis for processing the data, the individual objects to the processing of their data and there is no overriding legitimate interest to continue this processing;
- The Council is processing the personal data for direct marketing purposes and the individual objects to that processing;
- The Council has processed the personal data unlawfully;
- The personal data has to be deleted to comply with a legal obligation; and
- The Council has processed the personal data to offer information society services to a child.

The **Right to Erasure** does not apply when the processing of the personal data is necessary in the following circumstances:

- To exercise the right of freedom of expression and information;
- To comply with a legal obligation;
- For the performance of a task carried out in the public interest or in the exercise of official authority;
- For archiving purposes in the public interest, scientific or historical research purposes or statistical purposes where erasure is likely to render impossible or seriously impair the achievement of that processing; and
- For the establishment, exercise or defence of legal claims.

Although not likely to directly apply to the Council, legislation also specifies that the **Right to Erasure** will not apply in the case of special category data in the following circumstances for reasons of public health:

- If the processing is necessary for public health purposes in the public interest (e.g. protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices); and
- If the processing is necessary for the purposes of preventative or occupational medicine (e.g. where the processing is necessary for the working capacity of an employee; for medical diagnosis; for the provision of health or social care; or for the management of health or social care systems or services). This only applies where the data is being processed by or under the responsibility of a professional subject to a legal obligation of professional secrecy (e.g. a health professional).

If in some cases, the data cannot be deleted from backup systems immediately, the Council will restrict access to put it beyond use.

**8.1.4** **Right to Restriction of Processing:** Individuals have the right to request the Council to restrict the processing of their personal data in the following circumstances:

- The individual contests the accuracy of their personal data and the Council is verifying the accuracy of the data;
- The data has been unlawfully processed (i.e. in breach of the Lawfulness Principle) and the individual opposes erasure and requests restriction instead;
- The Council no longer needs the personal data but the individual needs the Council to keep it in order to establish, exercise or defend a legal claim; and
- The individual has objected to the processing for automated decision-making and the Council is considering whether its legitimate grounds override those of the individual.

**8.1.5** **Right to Data Portability:** Individuals have the right to receive personal data that they provided to the Council in a commonly used machine-readable format so that they can share it with a different organisation or use themselves. On request the Council may be obliged to share the personal data directly with the third party. The Council may turn the request down if it is not possible to comply.

**8.1.6** **Right to Object:** Individuals have the right to object to the processing of their personal data if the processing is based on legitimate interest and public interest grounds, including profiling.

**If the Council has a valid direct marketing consent in place and the individual objects, the direct marketing needs to stop immediately and a notification made not to use the personal data for that purpose again.** When communicating with individuals and in privacy notices it always has to be made clear that this right exists.

**8.1.7** **Right to Object to Automated Decision-making and Profiling:** Individuals have the right to not be subject to a decision based solely on automated processing which will have a legal or other effect on them. If the Council is required to perform credit checks or other forms of automated decision-making, it is usually done in the context of a

contract, the individual has given their explicit consent or the Council is required to do so by law. Individuals will still have the right to obtain human intervention, to express their point of view and to contest the decision.

### 8.2 Procedures for dealing with Data Subject Access Requests

#### 8.2.1 Response to Requests

When a request is received exercising any of the rights outlined in Section 8.1 the Data Protection Officer needs to be **informed immediately**.

Requests can be received in any format, including over the phone and via social media and do not have to be in written format and the Council cannot insist that it be provided in that format. **The formulation of the request may not always make it immediately clear that this is a Data Subject Access Request, it is therefore important to clarify.**

When an oral request is received it is helpful to explain that a written request might be easier to process and will therefore be dealt with faster as it will eliminate uncertainties or inaccuracies.

The person receiving the oral request needs to take down as much information as possible to enable the request to be actioned, including the contact details of the individual making the request. The individual making the request needs to be informed that the Council's Data Protection Officer will be in touch to action the request. If the person asks for a written request form, it is available as Appendix 5.

Once the request has been passed to the Data Protection Officer it will be assessed and managed to completion. The Data Protection Officer will establish the scope of the request to ensure the right data is retrieved and that the rights and freedoms of other individuals affected by the request are considered. If others are affected by the request, they will be consulted and a response provided in such a manner to ensure that their rights are also protected if required. In some cases, this might necessitate providing the information in redacted format.

**With all requests the identity of the individual making the request must be positively established before any information may be shared**. For more information on this please see Section 8.2.3 below.

The Council needs to be aware of the possibility that a fraudulent access request could be made that may result in a data breach if personal data is shared with someone other than a real data subject.

Correspondence for each request is filed together and each request is allocated a reference number and logged in the Data Subject Access Requests (DSAR) Register which is managed by the Data Protection Officer, refer Appendix 2.

#### 8.2.2 Response Timeframe

The Council is required by law to respond to the individual exercising their individual rights **without undue delay but in any event within one month of the receipt of the request. The Council will require a form of identification and once that is received the period starts**.

The Data Protection Officer will aim **to acknowledge the request via email (if possible) within 24 hours** and provide an indication of when a final response could be expected**. If more time is required due to the complexity of the request and the one-month deadline will not be met, the deadline can be extended by another two months. This will only happen in exceptional circumstances as the Council has a relatively small database and there is no large geographical spread.**

If more time is required the individual will be informed and provided with the reasons within the first one-month deadline period. The Council's expectation is that in most cases a response will be possible within one month.

The time limit is calculated from the day the request is received (whether the day is a working day or not) until the corresponding calendar date in the next month (e.g. request received on 3 September, so calendar response date is 3 October). If this is not possible because the following month is shorter (and there is no corresponding calendar date), the date for response is the last day of the following month. If the corresponding date falls on a weekend or a public holiday, the Council needs to respond by the next working day.

**The Council's aim is to complete the request as quickly as possible so as not to run the risk of missing the deadline. If the deadline is missed, the individual has the right to complain to the Information Commissioner's Office.**

### 8.2.3 Identification

**The Council is required to ensure that the identity of the individual making the request is established.** This is especially important if the request is made orally or through social media.

For the purpose of identification, the Council will accept a copy of the individual's driver's licence or passport. This can be provided via email, post or in person at the Parish Office.

If there is any doubt about the identity of the individual making the request, the Council can ask for additional proof of identification.

If the request is from a former employee or Councillor, identification might be sufficient if the individual is making the request from an email address on record or can provide information on their association with the Council that could only be known by the person in question (e.g. dates of start and end of association, employee number). If there are any doubts, the standard identification methods will be required.

If it is impossible to establish the identity of the person, the Council will be inclined to withhold the information and inform the individual of the reason**. A record of the decision-making process needs to be kept justifying this decision if the individual in question lodges a complaint with the Information Commissioner's Office.**

If the individual making the request is not the same as the person that the request is about (e.g. a solicitor or someone acting on their behalf) the Data Protection Officer will ask for a power of attorney or other proof of authority to act on behalf of the individual concerned.

**A copy of the identification method used will be kept on file in accordance with the Retention Policy and recorded in the Data Subject Access Request Register.**

### 8.2.4 Manner of Response

The Data Protection Officer will perform a thorough search of all Council files, both digital and paper, including archives. The results need to be checked to ensure that the data in question is not covered by an exemption. It is important to keep in mind that it is an offence to make any amendments with the intention of preventing its disclosure. The information provided will include all the aspects specified in Section 8.1.1 Right of Access.

Once the required redaction has been done, the copies are provided in such a way that they cannot be altered or changed (e.g. PDF). If the information contains codes or acronyms that will only be known inside Fair Oak and Horton Heath Parish Council and is unlikely to be understood by others, an explanation needs to be provided. If the request is received via email the normal response will be in that format, similarly with postal requests. If the response is sent via post, it needs to be in a manner that records receipt to enable the Council to verify that the individual making the request has received the information. If the copies are collected directly from the Parish Office a signature needs to be recorded confirming receipt.

# 9. Information Security and Breach Policy

Fair Oak and Horton Heath Parish Council has put appropriate technical and organisational measures in place for an organisation of its size to help safeguard the processing of personal data.

### 9.1 Information Security

To ensure the Council complies with the Security Principle all staff and Councillors are required to regularly change passwords with complexity enforced on all devices. Appropriate anti-virus and malware protection software must be installed on all devices and there should be an awareness of phishing scams. The access security of mobile devices provided by the Council should not be disabled.

Personal data should not be saved on any shared drives other than that of Fair Oak and Horton Heath Parish Council.

Where Council personal data is stored on home computers or mobile devices, the files and folders should have access controls enabled and only be accessible with a password. This is especially important where home devices are shared.

Only Fair Oak and Horton Heath Parish Council email addresses should be used for Parish Council business. If Councillors represent more than one Council, the business of the different Councils should be strictly separated to avoid creating a Joint Controller situation with the other Council. This will also enable the Council to meet its obligations to ensure that personal data is accurate and have access to all relevant data when a Data Subject Access Request is made. Personal and business email addresses should not be used for Parish Council business.

**If a Council-owned device with access to the Council's personal data is lost or stolen it should be reported to the Data Protection Officer immediately**. In the case of a mobile phone it is important to report the suspected loss immediately to instigate a temporary block on the device through the service provider. If the device is later recovered, the access can be restored.

If a lost or stolen device is privately-owned and has access to the Council's personal data, it is the responsibility of the owner to take immediate preventative action through their service provider and change passwords to block access to the device. The Data Protection Officer should be informed immediately to enable the Council to remotely disable access to the Council's documents.

**The Council will ensure that more than one designated person is registered with the Council's service providers (e.g. mobile operators) to ensure that action can be taken during a data breach if the main registered person is absent. This will include the person who is designated to act on data protection matters when the Data Protection Officer is unavailable or absent.**

When a device reaches the end of its useful life all personal data should be wiped and the device securely disposed of. This is especially important if it is a privately-owned device which is later sold. When staff leave the employ of the Council all devices must be returned before the last day of service and the user's private data deleted.

The Council will regularly update information security requirements to maintain security and take corrective action when a data breach occurs. This includes a Bring Your Own Device (BYOD) Acceptable Use Policy.

### 9.2 Breach Policy and Incident Response Strategy

**Fair Oak and Horton Heath Parish Council requires all staff and Councillors to report a data breach to the Data Protection Officer immediately.** This includes the loss of equipment containing or accessing personal data, the loss of paper files containing personal

data such as attendee lists at events or a list containing the personal data of residents, an email sent by mistake to the wrong person that contains personal data or accidentally sharing personal data.

**Any actions which could be regarded as the "accidental or unlawful destruction loss, alteration, unauthorised disclosure of, or access, to personal data transmitted, stored or otherwise processed" are considered data breaches.**

It is preferred that a proactive approach is taken if it is not clear whether an incident constitutes a data breach and it is therefore important to clarify with the Data Protection Officer immediately. Please provide as much information as possible.

When informed of a potential data breach, the Data Protection Officer will investigate and contact any processors involved to establish the likely risks to the individuals involved. Actions will be taken to minimise the risks to the individuals involved if possible.

If the investigation reveals that the personal data breach is unlikely to result in a risk to the rights and freedoms of the individuals affected or effective mitigating actions had been taken minimising the risks, the breach will be recorded in the Breach Register (Appendix 1) and remedial action will be taken to prevent a recurrence. In this case it will not meet the threshold for reporting the data breach to the Information Commissioner's Office.

Please note that risk to individuals is not only defined in terms of potential monetary loss but includes damage to reputation and harm (see Section 9.4).

### 9.3 Notifying the Regulator

If the Data Protection Officer finds that the breach is likely to result in a risk to the rights and freedoms of the individuals affected, the Information Commissioner's Office will be informed.

The notification must be done without undue delay but no later than **72 hours after having become aware of the breach**. The breach will also be recorded in the Breach Register.

The information provided to the Information Commissioner's Office will include the following:

- Description of the nature of the personal data breach including, where possible, the categories and approximate number of individuals impacted and the categories (e.g. special) and approximate number of personal data records concerned;
- The name and contact details of the Council's Data Protection Officer;
- A description of the likely consequences of the personal data breach; and
- A description of the measures taken or proposed to be taken by the Council to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

**The Data Protection Officer will report the breach and be the main contact. The Chair and Vice Chair of the Council will be kept informed of all developments.**

The document for completing a breach report via email is attached as Appendix 6. A breach can also be reported by calling the Information Commissioner's Office on 0303 123 1113.

### 9.4 Notifying the Individuals Concerned

If the investigation conducted by the Data Protection Officer reveals that the data breach is likely to result in a **high risk** to the rights and freedoms of those affected, the Data Protection Officer will inform those affected **without undue delay.**

**In assessing the likely risk it is important to keep in mind that damage could be physical, material, and non-material which might give rise to discrimination, identify theft or fraud, financial loss, damage to reputation, loss of confidentiality of personal data protected by professional secrecy, unauthorised reversal of pseudonymisation or other significant economic or social disadvantages.**

If the data was encrypted or measures had been taken after the event to ensure the high risks are no longer likely to materialise, it will not be necessary to inform the individuals affected.

The manner in which the individuals affected are informed is at the discretion of the Data Protection Officer and Council but if it is a very large number of individuals, a press statement might be required necessitating a strategy for handling the resultant enquiries.

# 10. Data Protection Roles, Record of Processing Activity and Performing a DPIA

The accountability framework that Fair Oak and Horton Heath Parish Council has put in place to comply with its data protection responsibilities assigns a number of duties.

## 10.1 Responsibilities of the Data Protection Officer

The Council has appointed the Clerk, as the Data Protection Officer.

The Data Protection Officer acts independently and does not receive instructions regarding the exercise of the tasks assigned to the role by law. The person holding the position shall not be dismissed or penalised for performing the tasks and reports directly to Full Council.

The duties of the Data Protection Officer are outlined in the legislation and include the following tasks at the Parish Council:

- To inform and advise the Data Controller (Full Council) and staff who carry out processing activities;
- To monitor compliance with the legislation, policies and procedures;
- To maintain an awareness programme, provide training and assign responsibilities;
- To provide advice on data protection impact assessments and monitor performance; and
- To cooperate with the Information Commissioner's Office and act as the contact point on issues when prior consultation is required.

In addition, at Fair Oak and Horton Heath Parish Council the Data Protection Officer has been assigned the following additional tasks:

- Updates the Data Protection Policy in consultation with Full Council;
- Maintains the legal Registers;
- Updates privacy notices, including for the website;
- Advises on changes to Cookie policies and notices;
- Keeps Full Council informed of legislative changes or interpretations and best practice advice from the Information Commissioner's Office; and
- Provides compliant marketing sign-up forms when required.

In the absence of the Clerk, the Council will assign another staff member to perform the duties of the Data Protection Officer. The staff member selected will be trained to perform the required duties, in particular in the handling of data breaches and Data Subject Access Requests.

## 10.2 Responsibilities of Full Council

Full Council is the Data Controller of Fair Oak and Horton Heath Parish Council and has overall governance responsibilities for the Council including compliance with data protection legislation.

The Data Controller has obligations set out in legislation which includes the implementation of "appropriate technical and organisational measures to ensure and to be able to demonstrate the processing is performed in accordance with the Regulation". This duty includes the implementation of appropriate data protection policies, adherence to approved codes or approved certification mechanisms to demonstrate compliance. Some sector specific codes of conduct might be introduced in future that can be applied to the Council.

Full Council sets the tone for how personal data is handled at the Council and communicates this privacy commitment to all staff and individuals the Council collects personal data from through privacy notices. It is the responsibility of Full Council to set the schedule for annual data protection audits and update reports on improvement programmes. Full Council also decides the parameters of the annual audits.

### 10.3 Responsibilities of Councillors

Councillors are also Data Controllers in their own right when they process personal data. This is most often the case when they are approached by residents for assistance or perform duties linked to their position on the Council. Councillors therefore also need to follow the data protection principles, lawful bases of processing and retention policy when processing personal data. The processing that Councillors do in the performance of their duties is recorded in the Council's Record of Processing Activity (RoPA) which also specifies the legal basis for the particular processing activity.

In line with the Transparency Principle, Councillors need to inform individuals how their data will be used including any sharing of personal data with colleagues and other Councils. A short paragraph in the email account of Councillors will explain this in brief and link to the Privacy Notice on the Council's website which will provide more detail including outlining individual rights and how to make a complaint.

Councillors must comply with the Council's Retention Schedule which outlines how long correspondence will be kept before it is securely destroyed or deleted. When a Councillor leaves the position, all records containing personal data need to be handed back to the Council or securely destroyed. Councillors leaving their positions must also hand over ongoing case work to a colleague for completion with the agreement of the individuals concerned.

Councillors who also serve on other Councils will use only their Fair Oak and Horton Heath Parish Council email account for parish business.

### 10.4 Record of Processing Activity (RoPA)

The Data Protection Officer keeps the Council's Record of Processing Activity Register (RoPA) in Appendix 3.

The Register records all the processing activity of the Council, provides the legal basis for each activity, specifies the categories of data and records recipients and transfers.

The RoPA is always kept up to date and is an important part of the accountability framework to provide evidence of the Council's compliance efforts.

The Register records at a minimum the following activities: collection, alteration, consultation, disclosure (including transfers), combination and erasure of personal data.

### 10.5 Data Protection Impact Assessment (DPIA)

The Data Protection Officer will carry out a Data Protection Impact Assessment if the Council intends to acquire new technology, move to a new database, change its CCTV operations or undertakes any new activities that could have a high impact on the rights and freedoms of the individuals involved. It is also required when a major change is made to an existing process that will impact the individuals concerned.

The DPIA will be carried out according to a prescribed format and will describe the nature, scope, context and purposes of the processing; assess the necessity, proportionality and compliance measures; identify and assess risks to individuals and identify any additional measures to mitigate the identified risks. In the event that the Council acquires new technology or instigates new processes that a DPIA finds will have a high risk to the individuals involved that cannot be adequately overcome by mitigating measures implemented, the Information Commissioner's Office should to be consulted.

### 10.6 Audits and Monitoring

An annual audit of documents and procedures will be carried out to ensure that policies and processes are still compliant and in line with current legislation and best practice. The results of the annual audits are presented to Full Council for action.

# 11. Privacy Notices

In accordance with the Right to Access and the Transparency and Fairness Principles the Council makes those individuals whom it collects personal data from aware of that fact and what their rights are regarding their personal data.

For these reasons the Council will have Fair Processing Notices (Privacy Notices) in place in the following instances:

- On the Council website;
- As part of contracts and agreements;
- Event registrations;
- Venue hire agreements;
- Staff contracts and Staff Handbook; and
- Marketing sign-up forms.

## 11.1 Information Provided

The Council will include the following details in privacy notices when it collects personal data:

- Council's name and details;
- Contact details of the Data Protection Officer;
- Why the personal data is collected and the Council's legal basis for doing so;
- When the Council uses legitimate interest as its legal basis it will be explained;
- Whether the data will be shared with other parties and identify them (or provide the categories);
- Whether the data will be sent to another country and the safeguards in place (the DPO can advise on this); and
- How long the data will be retained or provide a link to the Retention Policy.

The Council will also provide information on the rights of the individuals including the right to withdraw consent at any time and the right to complain to the Information Commissioner's Office.

If personal data is requested for legal or contractual reasons it will be make clear and what the implications are if this is not done.

The Council's website will also highlight any profiling done through a Cookie Notice.

## 11.2 Information Obtained Indirectly

When the Council has obtained personal data from another organisation (e.g. another Council), source or person, the individual affected will be informed when first contacting them and within one month unless the person already has the information, or the Council is legally required to collect the information.

The Council will provide all the information in Section 11.1 and in addition the following:

- Categories of data the Council holds including any sensitive and special category data (e.g. health); and
- Where the data was obtained from including public sources.

When the Council collects personal data or obtains it from another source and intends to use the data for another purpose rather than why it was collected in the first instance, the Council needs to have a valid legal basis for doing so and the individuals concerned informed.

# 12. Data Transfers, Processor and Joint Controller Responsibilities

Fair Oak and Horton Heath Parish Council does not transfer personal data to third countries as defined by data protection legislation. Should the situation change, the Council will put in place suitable safeguarding measures and the Data Protection Officer will advise on the most appropriate actions to take.

The Council currently uses the following processors:

a. RBS for financial transactions and burial records;
b. Microsoft Office 365 for storing information;
c. MailChimp for email marketing campaigns; and
d. WordPress and Smart Marketing for the website

These platforms and processors generally have adequate privacy and security procedures in place to safeguard the processing of the Council's personal data. The Council constantly reviews this position to ensure the ongoing safety of the personal data. If any concerns are raised or the Council becomes aware of reports of data breaches involving these service providers, the Council will take the necessary steps to protect the personal data they process.

The Council expects processors and joint controllers to comply with their obligations under data protection legislation to provide safeguards and report data breaches.

Agreements will be put in place with all new processors highlighting their data protection responsibilities regarding the Council's personal data.

At the end of a processing agreement the Council expects the data it provided to processors and joint controllers to be deleted from all databases unless there is a legal obligation to retain it for a specified period. Any paper files need to be securely destroyed.

# 13. Marketing

Direct marketing involves communications to an identified individual. Blanket marketing such as leaflets, advertisements and magazine inserts are not direct marketing. There is no restriction on sending solicited marketing.

In general, the Council relies on consent and legitimate interest as the valid legal bases for direct marketing and fundraising activities for events. Consent needs to meet the criteria set out in Section 5 and can be withdrawn at any time.

Fair Oak and Horton Heath Parish Council hosts a limited number of events and marketing is currently mainly done through the website, social media, newsletters and advertisements.

The Council intends to do more electronic marketing in future and will capture the consent required through compliant sign-up forms on the website and at events. The privacy notices on the sign-up forms will provide individuals with the required information in line with legislation and the consent will be stored in line with the Council's Retention Schedule.

Individuals will always be informed that they have the opportunity to unsubscribe at any time from marketing communications and how to go about removing their consent. When an individual requests to be removed from a marketing list, it will be done immediately, the person will be informed it had been done and precautions will be taken not to send any marketing communications to the same person by accident in future.

The Council does not buy or sell marketing lists. Should the position change in future a due diligence exercise will be conducted to ensure the existing consent is valid.

# 14. HR and Recruitment

Fair Oak and Horton Heath Parish Council has a legitimate interest to collect specific personal data for employment purposes and to meet its legal obligations.

## 14.1 Recruitment

Fair Oak and Horton Heath Parish Council recruits staff for permanent employment.

During the recruitment process and at the time of the first email exchange the Council will inform the applicants how their personal data will be used, including how long the details of unsuccessful applicants will be retained.

During the recruitment process the Council only collects information that is adequate, relevant and necessary for the purpose intended. When interviewing applicants, only information that is relevant to the position is collected. The interviewing panel will have access to information necessary for the purpose of making the selection but the information of applicants will not be made available outside of this panel unless there is a valid legal basis to do so. Access to the personal data of all applicants is restricted. The applicants are entitled to request a copy of their personal data which may include notes of the interview, including handwritten notes.

Background checks are only carried out if necessary for the role and the applicant is informed why it is necessary. If a negative outcome is received, the applicant has the opportunity to correct any inaccurate information. Access to the information is strictly on a need to know basis. The application forms, CVs and covering letters received during a recruitment process will be stored securely with limited access and retained according to the Retention Schedule.

If an applicant is successful, a personnel file will be opened and all documents created during the recruitment process will be securely filed in a secure filing cabinet or/and on password protected computer equipment. The retention period for the file will be for the employment period of the employee plus 7 years. If an applicant is unsuccessful or rejects a job offer, their data will be kept for 6 months and then destroyed. The name of the candidate, their address and email address will be retained for a period of 1 year. These retention periods will be communicated at first contact.

## 14.2 Processing personal data within the Council

Fair Oak and Horton Heath Parish Council complies with the Transparency Principle in the processing of the personal data of staff and Councillors. Whenever personal data is collected from employees and Councillors, they are informed about how their personal data will be used and how long it will be retained.

Staff will be informed of their privacy rights through the Staff Handbook/employment contract. Personal data of staff should only be collected for activities relating to the employee relationship and only what is needed for the specific purposes. If personal data will be used for a significantly different purpose, the employee has to be informed and the new purpose might require the consent of the employee. Where employees provide personal data about a family member or emergency contact, the employee has to confirm that they have informed the individual concerned and the reason. Consent must meet the requirement of being freely given.

In most cases only a minimum amount of information is required for absence, accident and sickness records. Access to these records is restricted to a need to know basis and will only be disclosed outside the Council if there is a legal obligation to do so, it is necessary for legal proceedings or the employee has been given a genuine choice about the sharing of the data with a third party for a particular purpose.

### 14.3 Monitoring

Employees can have a reasonable expectation of privacy at work. The monitoring of staff is likely to result in a high risk to their privacy and Fair Oak and Horton Heath Parish Council will in certain circumstances be required to carry out a Data Protection Impact Assessment to mitigate the risks. Staff have the right to be informed if they are subject to monitoring, why it is conducted, what kind of monitoring will take place, how it will be used and to whom it will be disclosed. Notification is required for monitoring activities such as email usage, geo-location device tracking, CCTV, internet and browsing activity tracking and the use of Council equipment. The Staff Handbook/employment contract will provide information on the Council's acceptable use policy and the existence of monitoring.

Covert monitoring is justified only in exceptional circumstances and will be specific and time limited. A valid legal basis needs to exist and the Chair and Vice Chair of the Council will need to approve the covert monitoring and set the limit, scale and scope.

### 14.4 Staff Performance

Fair Oak and Horton Heath Parish Council will ensure that information relating to performance improvement plans, grievances and dismissal is accurate and objective. Records relating to disciplinary and grievance matters are stored securely and only made available on a need to know basis. All records in the course of disciplinary and grievance proceedings will be accurate and sufficiently detailed to support any conclusions drawn. All HR and legal procedures will be followed while ensuring personal data is secure and only used for the purpose required and not in a way that is disproportionate to the matter under investigation.

### 14.5 Sharing Staff Data

Fair Oak and Horton Heath Parish Council will not share personal data of staff outside the Council except in the following circumstances:

- The employee has provided their feely given and informed consent (for example for a reference for their new employer). References will only be provided with the consent of the individual involved and will be according to the Council's HR policy;
- To protect an individual's vital interests;
- When required by law, regulation or court order;
- In connection with a legitimate request for assistance by the police or other law enforcement agency;
- To seek advice from the Council's solicitors;
- With respect to a legal dispute or administrative claim between the Council and a third party;
- To engage professional advisers;
- To meet the Council's contractual relationships; and
- To provide contact details for normal Council business such as enquiries from residents.

In all cases only the minimum information required for the purpose will be shared. If there is a likelihood of risk to the employee concerned the Data Protection Officer will be involved and if the risk is likely to be high, a Data Protection Impact Assessment will be conducted.

### 14.6 Pension, insurance and other benefits

When Fair Oak and Horton Heath Parish Council staff join a pension, health or other benefit scheme the employee will be informed what personal data is provided to the provider and how it will be used. The personal data required for this purpose will not be used or accessed for general employment purposes e.g. a medical record needed for a pension scheme will not be used in connection with eligibility for sick pay etc.

# 15. Policy Review

Fair Oak and Horton Heath Parish Council will review this Policy on an annual basis, the next review will take place in November 2020.

The Data Protection Officer will update the Policy when there are changes to legislation or new best practice advice is issued by the Information Commissioner's Office.

# Appendices

Appendix 1: Breach Register

Appendix 2: Data Subject Access Requests (DSAR) Register

Appendix 3: Record of Processing Activity (RoPA)

Appendix 4: Training Register

Appendix 5: Data Subject Access Request Form

Appendix 6: ICO Breach Reporting Form

Appendix 7: Retention Schedule