Title	Data Protection Policy	Warndon Parish Council

Owner (role)	The Clerk		
Reference & Version Number	V.1.1	Date:	23/04/2024

1. Purpose

1.1. This document sets out the obligations of Warndon Parish Council with regard to data protection and the rights of people with whom it works in respect of their personal data under the General Data Protection Regulation (GDPR), which came into force 25th May 2018.

1.2. This policy sets out how Warndon Parish Council is to treat personal data. This policy should be read in conjunction with all other supporting materials.

2. Scope of the Policy:

2.1. Warndon Parish Council is a data controller and/or data processor under the GDPR.

2.2. This policy is applicable to all personal data held by Warndon Parish Council whether the information is held or accessed on company premises, on removable devices and other portable media, or accessed via mobile or home working.

2.3. This policy covers all aspects of handling information, including (but not limited to):

2.3.1. Structured and unstructured (out of scope for GDPR) record systems – paper and electronic;
2.3.2. Transmission and receipt of information – fax, email, post and telephone;
2.3.3. Information systems managed and/or developed by, or used by Warndon Parish Council.

2.4. This policy covers all information systems, including cloud services by or on behalf of Warndon Parish Council, and any individual, directly or otherwise engaged by the council.

2.5. This policy applies to all councillors, employees, contractors, agency staff and third party suppliers and any other individuals with access to Warndon Parish Council information.

2.6. Councillors are responsible for developing and encouraging good information handling practices within Warndon Parish Council; responsibilities are set out in individual job descriptions.

2.7. Endorsement of this policy is mandatory at induction and should be refreshed through training annually.

2.8. More detailed specific duties with regards to handling of data are outlined in Section 12 below.

3. GDPR Context and Definitions

3.1. The General Data Protection Regulation supersedes the laws of individual Member States that were developed in compliance with the Data Protection Directive 95/46/EC. GDPR's purpose is to protect the "rights and freedoms" of natural persons (i.e. living individuals) and to ensure that personal data is not processed without their knowledge, and, wherever possible, that it is processed with their consent.

3.2. Definitions:

3.2.1. Material scope (Article 2) – the GDPR applies to the processing of personal data wholly or partly by automated means (i.e. by computer) and to the processing other than by automated means of personal data (i.e. paper records)

3.2.2. Territorial scope (Article 3) – the GDPR will apply to all controllers that are established in the EU (European Union) who process the personal data of data subjects, in the context of that establishment. It will also apply to controllers outside of the EU that process personal data in

order to offer goods and services, or monitor the behaviour of data subjects who are within the EU.

3.2.3. Establishment (Article 4) – the main establishment of the controller in the EU will be the place in which the controller makes the main decisions as to the purpose and means of its data processing activities. The main establishment of a processor in the EU will be its administrative centre. If a controller is based outside the EU, it will have to appoint a representative in the jurisdiction in which the controller operates to act on behalf of the controller and deal with supervisory authorities.

3.2.4. Personal data (Article 4) – any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

3.2.5. Special categories of personal data (Article 4) – personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

3.2.6. Data controller (Article 4) – the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

3.2.7. Data subject (Article 4) – any living individual who is the subject of personal data held by the organisation.

3.2.8. Processing (Article 4) – 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.

3.2.9. Profiling (Article 4) – is any form of automated processing of personal data intended to evaluate certain personal aspects relating to a natural person, or to analyse or predict that person's performance at work, economic situation, location, health, personal preferences, reliability, or behaviour. This definition is linked to the right of the data subject to object to profiling and a right to be informed about the existence of profiling, of measures based on profiling and the envisaged effects of profiling on the individual.

3.2.10. Personal data breach (Article 4) – 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. There is an obligation on the controller to report personal data breaches to the supervisory authority and where the breach is likely to adversely affect the personal data or privacy of the data subject.

3.2.11. Data subject consent (Article 4) - means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data.

3.2.12. Child – the GDPR defines a child as anyone under the age of 16 years old, although this may be lowered to 13 by Member State law. Where the child is below age where they can give consent under GDPR the consent of a parent or guardian will be required.

3.2.13. Third party (Article 4) – a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data.

3.2.14. Filing system (Article 4) – any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis.

4. Business Case

4.1. Warndon Parish Council views the correct and lawful handling of personal data as key to its success. The Council shall ensure that it handles all personal data correctly and lawfully.

4.2. Warndon Parish Council is committed to compliance with all relevant EU and Member State laws in respect of Data Protection and the protection of the "rights and freedoms" of individuals whose information the Council collects

and processes in accordance with the General Data Protection Regulation (GDPR).

4.3. The GDPR and this policy apply to all of Warndon Parish Council's personal data processing functions, including those performed on customers', clients', employees', suppliers' and partners' personal data, and any other personal data the organisation processes from any source.

4.4. Warndon Parish Council needs to process certain types of data about people with whom it deals in order to operate. This includes current, past and prospective employees, suppliers, clients and customers, and others with whom it communicates. In addition, the Council may occasionally be required by law to process personal information to comply with the requirements of governmental departments and other agencies. This personal data must be dealt with properly however it is collected, recorded and used whether on paper, held on or produced by a computer, or recorded on other material.

5. Data Protection Principles

5.1. Warndon Parish Council has established objectives for data protection and privacy.

5.2. GDPR requires us to handle the personal data in a safe, fair and lawful manner. The Council will ensure that it will treat all personal data lawfully and correctly.

5.3. To that end, Warndon Parish Council fully endorses and adheres to the Data Protection Principles set out in Article 5 of the GDPR. The Council's policies and procedures are designed to ensure compliance with the principles. These principles require that personal information we hold must be processed in the way set out in paragraphs 5.4 – 5.11:

5.4. <u>Personal data must be processed lawfully, fairly and transparently</u>

5.4.1. Lawful – identify a lawful basis before you can process personal data. These are often referred to as the "conditions for processing", for example consent.

5.4.2. Fairly – in order for processing to be fair, the data controller has to make certain information available to the data subjects as practicable. This applies whether the personal data was obtained directly from the data subjects or from other sources.

5.4.3. The GDPR has increased requirements about what information should be available to data subjects, which is covered in the 'Transparency' requirement.

5.4.4. Transparently – the GDPR includes rules on giving privacy information to data subjects in Articles 12, 13 and 14. These are detailed and specific, placing an emphasis on making privacy notices understandable and accessible. Information must be communicated to the data subject in an intelligible form using clear and plain language.

5.4.5. The Warndon Parish Council Privacy Policy is located at **https://warndonparishcouncil.org**

5.4.6. The specific information that must be provided to the data subject must, as a minimum, include:

5.4.6.1. the identity and the contact details of the controller and, if any, of the controller's representative;

5.4.6.2. the contact details of the Data Protection Officer (if applicable);

5.4.6.3. the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;

5.4.6.4. the period for which the personal data will be stored;

5.4.6.5. the existence of the rights to request access, rectification, erasure or to object to the processing, and the conditions (or lack of) relating to exercising these rights;

5.4.6.6. the categories of personal data concerned;

5.4.6.7. the recipients or categories of recipients of the personal data, where applicable;

5.4.6.8. where applicable, that the controller intends to transfer personal data to a recipient in a third country and the level of protection afforded to the data;

5.4.6.9. any further information necessary to guarantee fair processing.

5.5. <u>Personal data can only be collected for specific, explicit and legitimate purposes</u>

5.5.1. Data obtained for specified purposes must not be used for a purpose that differs from those formally notified to the supervisory authority as part of the Company's GDPR register of processing.

5.6. Personal data must be adequate, relevant and limited to what is necessary for processing

5.6.1. The Data Controller is responsible for ensuring that Warndon Parish Council does not collect information that is not strictly necessary for the purpose for which it is obtained.

5.6.2. All data collection forms (electronic or paper-based), including data collection requirements in new information systems, must include a fair processing statement or link to privacy statement and approved by the DPO/lead.

5.6.3. The DPO/lead will ensure that, on an annual basis all data collection methods are reviewed by audit experts to ensure that collected data continues to be adequate, relevant and not excessive.

5.7. Personal data must be accurate and kept up to date with every effort to erase or rectify without delay

5.7.1. Data that is stored by the data controller must be reviewed and updated as necessary. No data should be kept unless it is reasonable to assume that it is accurate.

5.7.2. The DPO/lead is responsible for ensuring that all staff are trained in the importance of collecting accurate data and maintaining it.

5.7.3. It is also the responsibility of the data subject to ensure that data held by the Council is accurate and up to date. Completion of a registration or application form by a data subject they will be required to confirm that their data is accurate.

5.7.4. Councillors, employees and others should be required to notify the Council of any changes in circumstance to enable personal records to be updated accordingly. It is the responsibility of the Council to ensure that any notification regarding change of circumstances is recorded and acted upon.

5.7.5. The DPO/lead is responsible for ensuring that appropriate procedures and policies are in place to keep personal data accurate and up to date, taking into account the volume of data collected, the speed with which

it might change and any other relevant factors. This should be accomplished by an audit.

5.7.6. On at least an annual basis, the Data Controller will lead review the retention dates of all the personal data processed by the Council, by reference to the data register, and will identify any data that is no longer required in the context of the registered purpose. This data will be securely deleted/destroyed in line with the Secure Disposal of Storage Media Procedure.

5.8. Personal data must be kept in a form such that the data subject can be identified only as long as is necessary for processing.

5.8.1. Where personal data is retained beyond the processing date, a lawful basis to retain this information needs to be in place, otherwise the data needs destroying. Where it is retained it should be minimised/ encrypted/ pseudonymised in order to protect the identity of the data subject in the event of a data breach.

5.8.2. Personal data will be retained in line with the retention schedule and, once its retention date is passed, it must be securely destroyed.

5.8.3. Records of destruction must be kept so as to satisfy the requirement to demonstrate accountability to the GDPR Article 5 principles.

5.8.4. The DPO/lead must specifically approve any data retention that exceeds the retention periods defined in retention schedule, and must ensure that the justification is clearly identified and in line with the requirements of the data protection legislation. This approval must be written.

5.9. Personal data must be processed in a manner that ensures the appropriate security

5.9.1. The DPO/lead will carry out a risk assessment taking into account all the circumstances of the Council's controlling or processing operations.

5.9.2. In determining appropriateness, the DPO/lead should also consider the extent of possible damage or loss that might be caused to individuals (e.g. Councillors, employees or customers) if a security breach occurs, the effect of any security breach on the Council itself, and any likely reputational damage including the possible loss of customer trust.

5.9.3. When assessing appropriate technical measures, the Data Controller will consider the following:

5.9.3.1. Password protection;
5.9.3.2. Automatic locking of idle terminals;
5.9.3.3. Removal of access rights for USB and other memory media
5.9.3.4. Virus checking software
5.9.3.5. Role-based access rights including those assigned to temporary employees
5.9.3.6. Encryption of devices that leave the organisations premises such as laptops
5.9.3.7. Security of local and wide area networks
5.9.3.8. Privacy enhancing technologies such as pseudonymisation and anonymisation;
5.9.3.9. Identifying appropriate international security standards relevant to the Parish Council.

5.9.4. When assessing appropriate organisational measures the Data Controller will consider the following:

5.9.4.1. The appropriate training levels throughout the Council;
5.9.4.2. Measures that consider the reliability of employees (such as references etc.);
5.9.4.3. The inclusion of data protection in employment contracts;
5.9.4.4. Identification of disciplinary action measures for data breaches;
5.9.4.5. Monitoring of councillors and employees for compliance with relevant security standards;
5.9.4.6. Physical access controls to electronic and paper based records;
5.9.4.7. Adoption of a clear desk policy;
5.9.4.8. Storing of paper based data in lockable fire-proof cabinets;
5.9.4.9. Restricting the use of portable electronic devices outside of the workplace;
5.9.4.10. Restricting the use of employee's own personal devices being used in the workplace;
5.9.4.11. Adopting clear rules about passwords;
5.9.4.12. Making regular backups of personal data and storing the media off-site;

5.9.4.13. The imposition of contractual obligations on the importing organisations to take appropriate security measures when transferring data outside the EEA.

5.9.5. These controls have been selected on the basis of identified risks to personal data, and the potential for damage or distress to individuals whose data is being processed.

5.10. <u>The controller must be able to demonstrate compliance with the GDPR's other principles (accountability)</u>

5.10.1. The GDPR includes provisions that promote accountability and governance. These complement the GDPR's transparency requirements. The accountability principle in Article 5(2) requires Warndon Parish Council to demonstrate that it complies with the principles and states explicitly that this is your responsibility.

5.10.2. Warndon Parish Council will demonstrate compliance with the data protection principles by implementing data protection policies, implementing technical and organisational measures, as well as adopting techniques such as data protection by design, DPIAs, breach notification procedures and breach incident response plans.

5.11. It is the responsibility of all Councillors and employees at the Council to be responsible for and able to demonstrate adherence to these principles at all times.

6. Data Subjects Rights

6.1. Data subjects have the following rights regarding data processing, and the data that is recorded about them:

6.1.1. To make subject access requests regarding the nature of information held and to whom it has been disclosed.

6.1.2. To prevent processing likely to cause damage or distress.

6.1.3. To prevent processing for purposes of direct marketing.

6.1.4. To be informed about the mechanics of automated decision-taking process that will significantly affect them.

6.1.5. To not have significant decisions that will affect them taken solely by automated process.

6.1.6. To sue for compensation if they suffer damage by any contravention of the GDPR.

6.1.7. To take action to rectify, block, erased, including the right to be forgotten, or destroy inaccurate data.

6.1.8. To request the supervisory authority to assess whether any provision of the GDPR has been contravened.

6.1.9. To have personal data provided to them in a structured, commonly used and machine-readable format, and the right to have that data transmitted to another controller.

6.2. To object to any automated profiling that is occurring without consent.

6.3. The Council ensures that data subjects may exercise these rights depending upon the local exemptions put in place by territory legislation.

6.4. The Data Controller shall ensure that a clear statement of how a data subject can access these rights should be displayed upon the privacy policy.

6.5. Data subjects may make data access requests as described in Subject Access Request Procedure. This procedure also describes how the Council will ensure that its response to the data access request complies with the requirements of the GDPR.

6.6. Data subjects have the right to complain to the Council related to the processing of their personal data, the handling of a request from a data subject and appeals from a data subject on how complaints have been handled in line with the Warndon Parish Council Complaints Procedure.

7. Security

7.1. All Councillors and employees are responsible for ensuring that any personal data that the Council holds and for which they are responsible, is kept securely and is not under any conditions disclosed to any third party unless that third party has been specifically authorised by the Council to receive that information and has entered into a confidentiality agreement.

7.2. All personal data should be accessible only to those who need to use it, and access may only be granted in line with the Access Control instructions, personal data should be treated with care and must be kept:

7.2.1. in a lockable room with controlled access; and/or

7.2.2. in a locked drawer or filing cabinet; and/or

7.2.3. if computerised, password protected in line with corporate requirements in the Access Control Policy.

7.2.4. stored on (removable) computer media which are encrypted in line with Secure Disposal of Storage Media

7.3. Care must be taken to ensure that PC screens and terminals are not visible except to authorised Councillors and employees of the Council of . All Click here to enter text.are required to enter into an Acceptable Use Agreement before they are given access to organisational information of any sort, which details rules on screen time-outs.

7.4. Manual records may not be left where they can be accessed by unauthorised personnel and may not be removed from business premises without explicit written authorisation. As soon as manual records are no longer required for day-to-day client support, they must be removed from secure archiving in line with the retention schedule.

7.5. Personal data should be deleted when there is no longer a use or lawful basis and should be deleted or disposed of in line with the retention schedule. Manual records that have reached their retention date are to be shredded and disposed of as 'confidential waste'. Hard drives of redundant PCs are to be removed and immediately destroyed before disposal.

7.6. Processing of personal data 'off-site' presents a potentially greater risk of loss, theft or damage to personal data. Staff must be specifically authorised to process data off-site by the Data Controller.

8. Disclosure of Data

8.1. Warndon Parish Council must ensure that personal data is not disclosed to unauthorised third parties which includes family members, friends, government bodies, and in certain circumstances, the Police. All Councillors

and employees should exercise caution when asked to disclose personal data held on another individual to a third party. It is important to bear in mind whether or not disclosure of the information is relevant to, and necessary for, the conduct of the Council's business.

8.2. All requests by third parties must be made in writing to the Data Controller and before any information is released a system of verification and consent to release exists.

8.3. All requests to provide data for one of these reasons must be supported by appropriate verification and all such disclosures must be specifically authorised by the Data Controller.

8.4. There are a number of options for verifying identity of the requestee.

8.5. You may either:

8.5.1. telephone the individual and ask them questions, based on the information you hold about them already, in order to confirm their identity; or

8.5.2. write to the individual and ask them to send a photocopy of their passport or driving licence and a recent utility bill to verify who they are and the address that they want the response sending to.

9. Retention and Disposal of Data

9.1. Warndon Parish Council shall not keep personal data in a form that permits identification of data subjects for longer a period than is necessary, in relation to the purpose(s) for which the data was originally collected.

10. Data Transfers

10.1. All exports of data from within the European Economic Area (EEA) to non-European Economic Area countries (referred to in the GDPR as 'third countries') are unlawful unless there is an appropriate "level of protection for the fundamental rights of the data subjects".

10.2. The transfer of personal data outside of the EEA is prohibited unless one or more of the four specified safeguards, or exceptions, apply:

10.3. An adequacy decision

10.3.1. The European Commission can and does assess third countries, a territory and/or specific sectors within third countries to assess whether there is an appropriate level of protection for the rights and freedoms of natural persons. In these instances no authorisation is required.

10.3.2. Countries that are members of the European Economic Area (EEA) but not of the EU are accepted as having met the conditions for an adequacy decision.

10.3.3. Lists of countries that currently satisfy the adequacy requirements of the Commission are published in the *Official Journal of the European Union. http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm*

10.4. The Privacy Shield

10.4.1. If Warndon Parish Council wishes to transfer personal data from the EU to an organisation in the United States it should check that the organisation is signed up with the Privacy Shield framework at the U.S. Department of Commerce. The US DOC is responsible for managing and administering the Privacy Shield and ensuring that companies live up to their commitments. In order to be able to certify, companies must have a privacy policy in line with the Privacy Principles e.g. use, store and further transfer the personal data according to a strong set of data protection rules and safeguards. The protection given to the personal data applies regardless of whether the personal data is related to an EU resident or not. Organisations must renew their "membership" to the Privacy Shield on an annual basis.

10.4.2. If they do not, they can no longer receive and use personal data from the EU under that framework.

10.5. Exceptions

10.5.1. In the absence of an adequacy decision, Privacy Shield membership, binding corporate rules and/or model contract clauses, a transfer of personal data to a third country or international organisation shall only take place on one of the following conditions:

10.5.2. The data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards;

10.5.3. The transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request;

10.5.4. The transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person;

10.5.5. The transfer is necessary for important reasons of public interest;

10.5.6. The transfer is necessary for the establishment, exercise or defence of legal claims; and/or

10.5.7. The transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent.

11. Warndon Parish Council Councillors and Employees; Obligations, Roles and Responsibilities:

11.1. The Clerk

11.1.1. The Clerk has ultimate responsibility for the Data Protection Policy within the Council. Implementation of, and compliance with this policy is delegated to the designated DPO/lead.

11.2. Data Protection Officer/lead

11.3. The DPO/lead must be a ????????, accountable to the Council for the management of personal data within the Council and for ensuring that compliance with data protection legislation and ensure that good practice can be demonstrated. with the policy.

11.3.1. The DPO/lead has overall responsibility for Data Protection and for overseeing the development, maintenance and monitoring of the Council's arrangements for Data Protection including:

11.3.1.1. The publishing, and administration of the Data Protection Policy;

11.3.1.2. The provision of data protection training for councillors and employees within the Council;

11.3.1.3. The development of best practice local guidelines; and

11.3.1.4. The carrying out of compliance checks to ensure adherence, throughout the Council, under GDPR.

12. <u>All Councillors and employees</u>

12.1. As a Councillor or an employee of the Council, you are subject to an obligation of confidentiality for all personal, sensitive and commercial information processed by the Council, and as such you must adhere to the GDPR and all confidentiality requirements, which form part of all employee Terms and Conditions of Employment and Council's obligations under the Freedom of Information Act 2000, the Data Protection Act 1998 and the Equality Act 2020.

12.2. While you are at work you may have access to information about Councillors, employees, residents, suppliers, and/or the Council. You may come in to contact with this type of information during the course of your work or simply see, hear or read something while you are working. Circumstances may occur where you believe that a duty of care, either to the councillor, employee, resident or supplier overrides the duty of confidentiality. This could be the case where serious harm for example in the case of suspected fraud may occur. In these circumstances you must discuss the matter with the Chair in the first instance, and/or, where practicable, obtain advice from the DPO. The discussion and outcome must be thoroughly documented and retained for future reference.

12.3. A copy of these documents must be provided to the Information Governance Manager for audit purposes. Otherwise, you must keep this information confidential.

12.4. Any unauthorised disclosure of information by a Councillor or employee may be considered as a disciplinary offence and could be subject to the Council's Disciplinary Procedures.

12.5. This policy, and its supporting standards and work instructions, are fully endorsed by the Data Controller

13. Our Processes/ Procedures:

13.1. Councillors and Employees:

13.2. Day to day:

13.2.1. Our Councillors and employees have a duty to make sure that they comply with the data protection principles, which are set out above in the Council's Data Protection Policy.
13.2.2. Individual Councillors and employees are responsible for ensuring that all data they are holding is kept securely.
13.2.3. Individual Councillors and employees are responsible for ensuring that paper records are destroyed securely, preferably shredded if no longer required or data transferred to electronic format.
13.2.4. Councillors and employees should also refer to and comply with the Council's additional internal guidance on the use of personal electronic devices for work purposes
13.2.5. Before processing any personal or sensitive data, all Councillors and employees should consider the checklist below.

13.3. Councillors and employees must consider the following factors/checklist when considering collecting personal data:

13.3.1. Do you really need to record the information?
13.3.2. Is the information 'personal' or is it special characteristic.
13.3.3. If it is a special category and is being transferred to a third party, do you have a secondary lawful basis?
13.3.4. Has the Data Subject been told that this type of data will be processed?
13.3.5. Are you authorised to collect / store / process the data?

13.3.6. Are you sure that the data is secure?

13.3.7. How long will you need to keep the data for, and what is the mechanism for review / destruction?

Reviewed at the Parish Council Meeting on