A picture containing shape

Description automatically generated

WHERSTEAD PARISH COUNCIL

DATA PROTECTION &

INFORMATION MANAGEMENT POLICY

Adopted at a meeting of Wherstead Parish Council on 8th March 2023

**DATA PROTECTION**

# ABOUT THIS POLICY

1.1 This policy outlines the standards Wherstead Parish Council (‘the Council’) intends to observe in relation to its compliance with the General Data Protection Regulation (GDPR) and subsequently revised UK Data Protection law.

1.2 The policy is applicable to all councillors and the Clerk/RFO.

1.3 The Council shall ensure that all users have access to the policy and fully understand its obligations.

1.4 This policy applies to all personal information created or held by the Council, in whatever format. This includes, but is not limited to paper, electronic, and film.

# RESPONSIBILITIES

2.1 To operate efficiently, the Council must collect and use information about people with whom it works. This may include members of the public, current, past, and prospective employees, customers, contractors, suppliers and partner organisations.

2.2 The Council regards the lawful and correct treatment of personal information as critical to its successful operations, maintaining confidence between the Council and those with whom it carries out business. The Council will, therefore, ensure that it treats personal information correctly in accordance with the law.

2.3 The Council as a whole is accountable for ensuring compliance with this policy.

2.4 All councillors and officers who hold or collect personal data are responsible for compliance with data protection legislation and must ensure that personal and/or sensitive information is kept and processed in accordance with this policy.

# BREACH OF THIS POLICY

3.1 Breach of this policy by the Clerk/RFO may result in disciplinary action in accordance with the Council’s disciplinary procedures and, in certain circumstances may be considered to be gross misconduct, resulting in dismissal. It should also be noted that breach of the policy could also lead to criminal or civil action if illegal material is involved, or legislation is contravened. Councillors found to be in breach of this policy may also be deemed to have breached the Code of Conduct and referred to the District Council’s Monitoring Officer.

# INFORMATION SHARING

4.1 The Council may share information when it is in the best interests of the data subject and when failure to share data may carry risks to vulnerable groups and individuals.

4.2 Information must always be shared in a secure and appropriate manner and in accordance with the information type. The Council will be transparent and as open as possible about how and with whom data is shared; with what authority; and for what purpose; and with what protections and safeguards.

4.3 Any Councillor or officer dealing with telephone enquiries must be careful about disclosing personal information held by the Council. In order to manage this the enquirer will be asked to put their request in writing in the first instance.

# INDIVIDUALS’ RIGHTS

5.1 An individual may request a copy of any data held about them, or information about the reasons for which it is kept and processed. This is called a Subject Access Request (SAR). Information on how an individual can make a SAR can be found on the Wherstead Parish Council web page: Wherstead.onesuffolk.net.

# DISCLOSURE OF PERSONAL INFORMATION TO THIRD PARTIES

6.1 Personal data can only be disclosed about a third party in accordance with the Data Protection Act 2018.

6.2 If a user believes it is necessary to disclose information about a third party to a person requesting data, they must seek specialist advice before doing so.

# BREACH OF INFORMATION SECURITY

7.1 The Council understands the importance of recognising and managing information security incidents. This occurs when data or information is transferred to somebody who is not entitled to receive it. It includes losing data or theft of information, unauthorised use of the Council’s system to process or store data by any person or attempted unauthorised access to data or information regardless of whether this was successful or not.

7.2 All users have an obligation to report actual or potential data protection compliance failures as soon as possible and take immediate steps to minimise the impact and to assist with managing risk. The Council will fully investigate both actual and potential failures and take remedial steps, if necessary, maintain a register of compliance failures. If the incident involves or impacts personal data, it must be reported to the ICO within 72 hours.

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

# IT AND COMMUNICATIONS SYSTEMS

8.1 The Council’s IT and communications systems are intended to promote effective communication and working practices. This policy outlines the standards users must observe when using these systems and the action the Council will take if users breach these standards.

8.2 Breach of this policy may be dealt with under the Council’s Disciplinary Procedure and, in serious cases, may be treated as gross misconduct.

# EQUIPMENT SECURITY AND PASSWORDS

9.1 Councillors and officers are responsible for the security of the equipment allocated to them, and must not allow it to be used by anyone other than in accordance with this policy. Passwords must be set on all IT equipment and passwords must remain confidential and be changed regularly.

9.2 Users must only log onto Council systems using their own username and password. Users must not use another person’s username and password or allow anyone else to log on using their username and password.

# SYSTEMS AND DATA SECURITY

10.1 Users should not delete, destroy, or modify existing systems, programs, information or data (except as authorised in the proper performance of their duties).

10.2 Users must not download or install software from external sources unless previously agreed by the Council. Downloading unauthorised software may interfere with the Council’s systems and may introduce viruses or other malware.

10.3 Users should exercise particular caution when opening unsolicited e-mails from unknown sources. If an e-mail looks suspicious do not reply to it, open any attachments, or click any links in it.

# E-MAIL

11.1 Users should adopt a professional tone and observe appropriate etiquette when communicating with third parties by e-mail.

11.2 It should be noted that e-mails can be used in legal proceedings and that even deleted e-mails may remain on the system and be capable of being retrieved.

11.3 Users must not send abusive, obscene, discriminatory, racist, harassing, derogatory, defamatory, pornographic, or otherwise inappropriate e-mails.

11.4 For the purposes of council business, users must use a designated email account in order to receive or send email correspondence.

# USING THE INTERNET

12.1 Users should not access any web page or download any image or other file from the internet which could be regarded as illegal, offensive, in bad taste or immoral. Even web content that is legal in the UK may be in sufficient bad taste to fall within this prohibition. As a general rule, if any person (whether intended to view the page or not) might be offended by the contents of a page, or if the fact that our software has accessed the page or file might be a source of embarrassment if made public, then viewing it will be a breach of this policy.

# PROHIBITED USE OF COUNCIL SYSTEMS

13.1 Misuse or inappropriate internet use will be dealt with under the Council’s Disciplinary Procedure. Misuse of the internet can in some cases be a criminal offence.

13.2 Creating, viewing, accessing, transmitting, or downloading any of the following material will usually amount to gross misconduct (this list is not exhaustive):

1. pornographic material (that is, writing, pictures, films and video clips of a sexually explicit or arousing nature);

1. offensive, obscene, or criminal material or material which is liable to cause embarrassment to us or our local community.

1. a false and defamatory statement about any person or organisation.

1. material, which is discriminatory, offensive, derogatory or may cause embarrassment to others (including material which breaches our Equal Opportunities Policy or our Anti-harassment and Bullying Policy);

1. confidential information about the Council or any of our staff or our community (except as authorised in the proper performance of your duties).

1. unauthorised software.

1. any other statement which is likely to create any criminal or civil liability; or

1. music or video files or other material in breach of copyright.

# SOCIAL MEDIA

14.1 This policy is in place to minimise the risks to our Council through use of social media.

14.2 This policy deals with the use of all forms of social media and all other social networking sites, internet postings and blogs. It applies to use of social media for Council purposes as well as personal use that may affect our business in any way.

# PROHIBITED USE

15.1 Users must avoid making any social media communications that could damage the Council’s interests or reputation, even indirectly.

15.2 Users must not use social media to defame or disparage Wherstead Parish Council, Council staff or any third party; to harass, bully or unlawfully discriminate against staff or third parties; to make false or misleading statements; or to impersonate colleagues or third parties.

# GUIDELINES FOR RESPONSIBLE USE OF SOCIAL MEDIA

16.1 Users should make it clear in social media postings, or in their personal profile, that they are speaking on their own behalf.

16.2 Be respectful to others when making any statement on social media and be aware that they are personally responsible for all communications which will be published on the internet for anyone to see.

16.3 A data protection breach may result in disciplinary action up to and including dismissal.

16.4 Members or staff may be required to remove any social media content that the Council believes constitutes a breach of this policy. Failure to comply with such a request may in itself result in disciplinary action.

# RECORDS MANAGEMENT

17.1 It is necessary for the Council to retain a number of data sets as part of managing council business. The Council shall apply the following framework:

|  |  |  |
| --- | --- | --- |
| DOCUMENT | MINIMUM RETENTION  PERIOD | REASON |
|  Minute books | Indefinite | Archive |
|  Receipt and payment account(s) | 6 years | Management |
|  Receipt books of all kinds | 6 years | VAT |
|  Bank statements, including deposit/savings accounts | Last completed audit year | Audit |
|  Bank paying-in books | Last completed audit year | Audit |
|  Cheque book stubs | Last completed audit year | Audit |
|  Paid invoices | 6 years | VAT |
|  Paid cheques | 6 years | Limitation Act 1980 (as amended) |
|  VAT records | 6 years | VAT |
|  Petty cash | 6 years | Tax, VAT, Limitation Act 1980  (as amended) |
|  Insurance policies | While valid | Management |