Occold Parish Council

DATA PROTECTION & INFORMATION MANAGEMENT POLICY

DATA PROTECTION

1 ABOUT THIS POLICY

1.1 This policy outlines the standards Occold 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 any employees, partners, voluntary groups, third parties and agents authorised by them.

1.3 The Council shall ensure that all users fully understand its obligations and have undertaken the necessary training to demonstrate compliance with this policy.

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, mail, microfiche and film.

2 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. The day-to-day responsibilities are delegated to the Clerk, who will undertake information audits and manage the information collected by the Council including the issuing of privacy notices, dealing with requests and complaints raised and the safe disposal of information.

2.4 Councillors who process personal data on an individual basis and are not acting on behalf of the council are likely to be considered data controllers and therefore required to notify the Information Commissioner's Office.

2.5 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.

3 BREACH OF THIS POLICY

3.1 Breach of this policy may result in diciplinary action in accordance with the Council's Conduct or Capability procedures and, in certain circumstances may be considered to be gross misconduct, resulting in dismissal.

3.2 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.

4 PRIVACY BY DESIGN

4.1 The GDPR requires data controllers to put measures in place to minimise personal data processing and that they only process data that is necessary for the purposes of processing and stored for as long as is necessary.

4.2 The Council will have the appropriate measures in place to determine the basis for lawful processing and will undertake risk assessments to ensure compliance with the law. These measures include the use of Data Protection Impact Assessments (DPIAs).

5 CONTRACTS

5.1 Data protection law places requirements on both the Council and its suppliers to ensure the security of personal data, and to manage individuals' privacy rights. This means that whenever the Council uses a supplier to process individuals' data on its behalf it must have a written contract in place.

5.2 The law sets out what needs to be included in the contract so that both parties understand their responsibilities and liabilities.

5.3 The Council is liable for its compliance with data protection law and must only appoint suppliers who can provide 'sufficient guarantees' that the requirements of the law will be met, and the rights of individuals protected.

5.4 If a contractor, partner organisation or agent of the Council is appointed or engaged to collect, hold, process or deal with personal data on behalf of the council, or if they will do so as part of the services they provide to the Council, the relevant lead Councillor or Council officer must ensure that personal data is managed in accordance with data protection law and this Policy.

5.5 Security and data protection requirements must be included in any contract that the agent, contractor or partner organisation enters into with the Council and reviewed during the contract's life cycle.

5.6 Council officers will use the appropriate processes, templates and DPIAs when managing or issuing contracts.

6 INFORMATION SHARING

6.1 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.

6.2 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.

6.3 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 enquirier will be asked to put their request in writing in the first instance.

7 INDIVIDUALS' RIGHTS

7.1 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 in the Subject Access Request Policy

7.2 Individuals also have other rights under the Data Protection Act 2018 which are set out in the Council's privacy notices. The Council must respond to individuals exercising their rights within one month.

8 DISCLOSURE OF PERSONAL INFORMATION TO THIRD PARTIES

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

8.2 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.

9 BREACH OF INFORMATION SECURITY

9.1 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.

9.2 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.

10 IT AND COMMUNICATIONS SYSTEMS

10.1 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.

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

11 EQUIPMENT SECURITY AND PASSWORDS

11.1 Councillors and officers are responsible for the security of the equipment allocated to or used by 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.

11.2 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.

12 SYSTEMS AND DATA SECURITY

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

12.2 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.

13 E-MAIL

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

13.2 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.

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

13.4 For the purposes of council business, users must use a designated email account (or only use the email account provided) in order to receive or send email correspondence.

14 USING THE INTERNET

14.1 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.

15 PROHIBITED USE OF COUNCIL SYSTEMS

15.1 Misuse or excessive personal use of our telephone or e-mail system 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.

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

(a) pornographic material (that is, writing, pictures, films and video clips of a sexually explicit or arousing nature);
(b) offensive, obscene, or criminal material or material which is liable to cause embarrassment to us or our local community;
(c) a false and defamatory statement about any person or organisation;
(d) 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);
(e) confidential information about the Council or any of our staff or our community (except as authorised in the proper performance of your duties);
(f) unauthorised software;
(g) any other statement which is likely to create any criminal or civil liability; or
(h) music or video files or other material in breach of copyright.

6 SOCIAL MEDIA

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

16.2 Users must not use social media to defame or disparage us, 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.

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

16.4 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.

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

16.6 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.

17 BRING YOUR OWN DEVICE (BYOD)

The Council must take appropriate technical and organisational measures against accidental loss or destruction of or damage to personal data. Councillors using their own devices raises a number of data protection concerns due to the fact that these are owned by the user rather than the data controller. The risks the controller needs to assess are:

- The type of data held.
- Where the data may be stored.
- How the data is transferred.
- Potential data leakage.
- Blurring of personal and business use.
- The device's security capacities.
- What to do if the person who owns the device leaves the Council and
- How to deal with the loss, theft, failure and support of a device.

Councillors and officers using their own devices shall have the following responsibilities:

- Users will enable a security pin to access their device and an automatic lock every 5 minutes requiring re-entry of the pin.
- Users will ensure security software is set up on their device and kept up to date.
- Users will delete all Council business from their device on leaving their post

18 RECORDS MANAGEMENT

18.1 It is necessary for the Council to retain a number of data sets as part of managing council business. This policy applies to Occold parish council (OPC) and covers all records and

documentation, whether analogue or digital and are subject to the retention requirements of this policy.

18.2 For the purpose of this policy, the terms ‘documents’ and ‘records’ include information in both hard copy and electronic form and have the same meaning whether referred to as documents or documentation.

18.3 This policy will also aid paper records and electronic data storage issues identified and will eliminate the need to retain paper and electronic records unnecessarily. OPC will ensure that information is not kept longer than is necessary and will retain the minimum amount of information that it is required to hold to meet its statutory functions and the provision of its services.

18.4 Anything that is no longer of use or value can be destroyed but if the council is in any doubt it will seek advice from Suffolk Association of Local Councils (SALC) and retain that document until that advice has been received. Documents of historical importance, if not retained by the council, will be offered first to the county record office.

18.5 Planning Papers are no longer issued and available electronically via the Babergh and Mid Suffolk District Council Planning Portal.

18.6 Insurance policies and significant correspondence will be kept for as long as it is possible to make a claim under the policy.

Article 4 of the Employer’s liability (Compulsory Insurance) regulations 1998 (si 2753) requires that local councils, as employers, retain certificates of insurance against liability for injury or disease to their employees arising out of their employment for a period of 40 years from the date on which the insurance is commenced or renewed.

18.7 Circulars and legal topic notes from SALC, NALC and other bodies such as principal authorities will be retained electronically as long as the information contained therein is useful and relevant.

18.8 Correspondence will be retained electronically for 2 years or as long as the matter contained therein is still of interest or use to the council and or the parish.

18.9 Personnel matters **-** Article 5 of GDPR provides “personal data must be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.” This policy will ensure that necessary records, documents and electronic data of OPC are adequately protected, archived and disposed of at the correct retention period, and to provide all staff with clear instructions regarding the appropriate retention and disposal of such documentation.

19 RETENTION OF DOCUMENTS FOR LEGAL PURPOSES

19.1 Most legal proceedings are governed by 'the limitation acts' which state that legal claims may not be commenced after a specified period. the specified period varies, depending on the type of claim in question. The table below sets out the limitation periods for the different categories of claim.

Claims under category	Limitation period
Negligence (and other torts)	6 years
Defamation	1 year
Contract	6 years
Leases	12 years
Sums recoverable by statute	6 years
Personal injury	3 years
To recover land	12 years
Rent	6 years
Breach of trust	None

19.2 If a type of legal proceeding falls into two or more categories, the documentation will be kept for the longer of the limitation period. As there is no limitation period in respect of trust, the council will retain all trust deeds and schemes and other similar documentation.

20. DISPOSAL OF DOCUMENTS OR DOCUMENTATION

20.1 Any record containing confidential information must either be disposed of in a confidential waste bin or shredded using a cross-cut shredder. Disposal of documents that do not contain confidential information may be disposed of in the normal way or recycled. Computer files will be deleted bth from the computer file and the trash bin.

20.2 Transfer of document to external body - this method of disposal will be relevant where documents or records are of historic interest and/or have intrinsic value. such a third party could be the county archivist or a local museum.

21. DISPOSAL OF ELECTRICAL HARDWARE

21.1 IT equipment and devices that have the ability and capability to store personal data include: Laptops, Mobile phones, Multi-functional devices – printers / scanners, Servers , USB memory sticks and external hard drives. IT equipment disposal must be managed by the Chair and Clerk ensuring all memory is destroyed.

21.2 All computer equipment, recycling or refurbishing must be disposed of in accordance with the waste electric and electronic equipment regulations 2013.

Appendix 1 - Retention of documents required for the audit of parish councils

Document	Minimum retention period	Reason
Minutes books	indefinite	Archive
Receipt and payment account(s)	indefinite	Archive
Receipt books	6 years	VAT
Bank statements/paying in books/cheque stubs	last completed audit year	Audit
Supplier contracts	6 years	limitation act 1980 (as amended)
Quotations/tenders	12 years	limitation act 1980 (as amended)
Paid invoices	6 years	Vat
Paid cheques	6 years	limitation act 1980 (as amended)
VAT records	6 years	Vat
Timesheets	last completed audit year	Audit
Insurance policies	while valid	management
Certificates for insurance against liability for employees	40 years from date on which insurance commenced or was renewed	the employers' liability (compulsory insurance), regulations 1998 (si 2753), management
Title deeds, leases, agreements, contracts	indefinite	audit, management
Staff attendance records	indefinite	health & safety act 1974
Members allowances registers	6 years	limitation act 1980 (as amended)

Appendix 2 - Retention of documents required relating to information technology

Document	Minimum retention period	Reason
Email	2 years	to satisfy customer complaints
Electronic back up	12 months	to protect records from loss, destruction or falsification
Electronic files	3 years from date last used	to protect records from loss, destruction or falsification
All portable / removable storage media	At end of work cycle / project	data shall be copied or stored on removable media only by authorised users in the performance of official duties