

HUNDON PARISH COUNCIL

Data Protection and Information Management Policy

Updated May 2021

Data Protection

1. About this Policy

- 1.1 This policy outlines the standards Hundon 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 Council Manager, 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. The Council notes that from the 1st May 2019, the Data Protection (Charges and Information) (Amendment) Regulations 2019 came into force. The Regulations state that elected representatives are exempt from paying a fee.
- 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 disciplinary action in accordance with the Council's Code of Conduct procedure 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.

4. Privacy by Design

4.1 The GDPR requires data controllers to put measures in place to minimize 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 organization 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 interest 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 enquirer 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 on the Council's website www.hundonparishcouncil.co.uk
- 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 understand 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 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 and 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. I.T and Communication Systems

- 10.1 The Council's I.T 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 and Security 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 I.T 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 name 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 must not download or install software from external sources. Downloading unauthorised software may interfere with the Council's systems and may introduce viruses or other malware.
- 12.3 Users must not attach any device or equipment including mobile phones, tablet computers or USB storage devices to the Council's systems.
- 12.4 Users should exercise particular caution when opening unsolicited emails from unknown sources. If an email looks suspicious, do not reply to it, open any attachments or click any links in it.
- 12.5 Users must inform the Council Manager immediately if they suspect a computer may have a virus.

13. Email

- 13.1 Users should adopt a professional tone and observe appropriate etiquette when communicating with third parties by email.
- 13.2 It should be noted that emails can be used in legal proceedings and that even deleted emails 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 emails.
- 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 the Council's 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. Social Media

- 15.1 This policy is in place to minimise the risks to our Council through use of social media.
- 15.2 This policy deals with the use of all forms of social media including Facebook, LinkedIn, Twitter, Google+, Wikipedia, Instagram 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 the Council's business in any way.

16. Prohibited Use

- 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 this Council, its 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 Any misuse of social media should be reported to the Council Manager.

17. Guidelines for Responsible Use of Social Media

- 17.1 Users should make it clear in social media postings, or in their personal profile, that they are speaking on their own behalf.
- 17.2 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.
- 17.3 A data protection breach may result in disciplinary action up to and including dismissal.
- 17.4 Members of 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.

18. Bring your Own Device (BOYD)

This 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 not lend their device to anybody;
- Users will inform the Council should they lose, sell, recycle or change their device;
- Users will take adequate security precautions to access their device.
- Users will ensure security software is set up on their device and kept up to date; and
- Users will not use their device to store Council emails, files and data.

19. Records Management

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

Document	Minimum Period	Reason
MINUTES		
Approved minutes	Indefinite	Archive
Draft/rough/notes of minutes taken at meetings	Until minutes are approved	Management
FINANCE		
Receipt and Payment Accounts	Indefinite	Archive
Paid invoices	6 years	VAT
VAT records	6 years	VAT
Bank Statements	6 years*	Audit
Paying in books	6 years*	Audit
Cheque stubs	6 years*	Audit
Scales of fees and charges	5 years	Management
Members allowances register	6 years	Tax, Statute of Limitations

PLANNING

Permissions	6 years	Compliance
Permissions - on appeal	Indefinite	Precedent
Permissions - commercial or development	Indefinite	Future compliance
Refusals	2 years	Appeals

INSURANCE

Insurance policies	2 years	Management
Certificates of Employers' Liability Insurance	40 years	Limitation period

OTHER

Quotations and tenders	12 years /indefinite	Statute of Limitations
Title deeds, leases, agreements, contracts	Indefinite	Audit, Management
Routine correspondence, papers & emails		Retain as long as useful
Notes from meetings	Until minutes are confirmed	Minutes are signed