

# **Bramfield and Thorington Parish Council**

## **DATA PROTECTION & INFORMATION MANAGEMENT POLICY**

## **DATA PROTECTION**

### **1 ABOUT THIS POLICY**

**1.1** This policy outlines the standards Bramfield and Thorington Parish Council ('the Parish Council') it 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 Parish 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 Parish 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 Parish Council regards the lawful and correct treatment of personal information as critical to its successful operations, maintaining confidence between the Parish Council and those with whom it carries out business. The Parish Council will, therefore, ensure that it treats personal information correctly in accordance with the law.

**2.3** The Parish 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 Parish 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 Parish 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** Malicious breach of this policy 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.

### **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 Parish 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 Parish Council and its suppliers to ensure the security of personal data, and to manage individuals' privacy rights. This means that whenever the Parish 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 Parish 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 Parish 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 Parish Council, the relevant lead Councillor or Parish 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 Parish Council and reviewed during the contract's life cycle.

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

## **6 INFORMATION SHARING**

**6.1** The Parish 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 Parish 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 Parish 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). An individual can make a SAR to the Clerk or Chair of the Parish Council.

**7.2** Individuals also have other rights under the Data Protection Act 2018 which are set out in the Parish Council's privacy notices. The Parish 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 Parish 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 Parish 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 Parish 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 Parish 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 Parish Council will take if users breach these standards.

**10.2** Malicious breach of this policy may be dealt with under the Parish 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 if the passwords become compromised.

**11.2** Users must only log onto Parish 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 must be very careful to download or install software from external sources. Downloading software may interfere with the Council's systems and may introduce viruses or other malware. The system should have anti-virus and anti-malware installed on the system.

**12.3** Users must check that any device or equipment including mobile phones, tablet computers or USB storage devices are checked for viruses and malware before connecting to the system.

**12.4** 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.

**12.5** Users must inform Clerk immediately if they suspect a computer may have a virus.

## **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 Parish Council business, users must use a designated email accounts (or only use the email account provided) in order to receive or send email correspondence.

## **14 USING THE INTERNET**

**14.1** Users should not maliciously 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.

As a general rule, if any person (whether intended to view the page or not) might be reasonably 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** Maliciously 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 reasonably cause embarrassment to others (including material which breaches our Equal Opportunities Policy or our Anti-harassment and Bullying Policy);

**(e)** confidential information about the Parish 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.

## **16 SOCIAL MEDIA**

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

## **17 PROHIBITED USE**

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

**17.2** Users must not use social media to defame or disparage us, Parish 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.

**17.3** Any misuse of social media should be reported to the Clerk or chair of the Council.

## **18 GUIDELINES FOR RESPONSIBLE USE OF SOCIAL MEDIA**

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

**18.2** 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.

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

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

## **19 BRING YOUR OWN DEVICE (BYOD)**

The Parish 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 Parish 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 Parish Council should they lose, sell, recycle or change their device.
- 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 not use their device to store Parish Council emails, files and data.

## 20 RECORDS MANAGEMENT

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

DOCUMENT	MINIMUM RETENTION PERIOD	REASON
<input type="checkbox"/> Minute books	Indefinite	Archive
<input type="checkbox"/> Scales of fees and charges	6 years	Management
<input type="checkbox"/> Receipt and payment account(s)	Indefinite	Archive
<input type="checkbox"/> Receipt books of all kinds	6 years	VAT
<input type="checkbox"/> Bank statements, including deposit/savings accounts	Last completed audit year	Audit
<input type="checkbox"/> Bank paying-in books	Last completed audit year	Audit
<input type="checkbox"/> Cheque book stubs	Last completed audit year	Audit
<input type="checkbox"/> Quotations and tenders	6 years	Limitation Act 1980 (as amended)
<input type="checkbox"/> Paid invoices	6 years	VAT
<input type="checkbox"/> Paid cheques	6 years	Limitation Act 1980 (as amended)
<input type="checkbox"/> VAT records	6 years generally but 20 years for VAT on rents	VAT
<input type="checkbox"/> Petty cash, postage and telephone books	6 years	Tax, VAT, Limitation Act 1980 (as amended)
<input type="checkbox"/> Timesheets	Last completed audit year 3 years	Audit (requirement) Personal injury (best practice)

<input type="checkbox"/> Wages books	12 years	Superannuation
<input type="checkbox"/> Insurance policies	While valid	Management
<input type="checkbox"/> 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.
<input type="checkbox"/> Investments	Indefinite	Audit, Management
<input type="checkbox"/> Title deeds, leases, agreements, contracts	Indefinite	Audit, Management
<input type="checkbox"/> Members allowances register	6 years	Tax, Limitation Act 1980 (as amended)
<b>For Halls, Centre, Recreation Grounds</b>		
<ul style="list-style-type: none"> <li>▪ application to hire</li> <li>▪ lettings diaries</li> <li>▪ copies of bills to hires</li> <li>▪ record of tickets issued</li> </ul>	6 years	VAT
<b>For Allotments</b>		
<input type="checkbox"/> Tenancy Agreement, register and plans	Indefinite	Audit, Management
<b>For Burial Grounds</b>		
<ul style="list-style-type: none"> <li>▪ register of fees collected</li> <li>▪ register of burials</li> <li>▪ register of purchased graves</li> <li>▪ register/plan of grave spaces</li> <li>▪ register of memorials</li> <li>▪ applications for interment</li> </ul>	Indefinite	Archives, Local Authorities Cemeteries Order 1977 (SI. 204)

<ul style="list-style-type: none"><li>▪ applications for right to erect memorials</li><li>▪ disposal certificates</li><li>▪ copy certificates of grant of exclusive right of burial</li></ul>		
---	--	--