HAWSTEAD PARISH COUNCIL

DATA PROTECTION AND INFORMATION MANAGEMENT POLICY

Adopted 28 May 2020

Last reviewed January 2026

Review date May 2027

Hawstead Parish Council | Brokesbourne Stanningfield Road, Great Whelnetham Suffolk IP30 0TY| catherine.hibbert@hawstead-parish-council.co.uk | 01284 388504

DATA PROTECTION

1 ABOUT THIS POLICY

1.1 This policy outlines the standards Hawstead Parish Council ('the 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 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 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 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 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 SAR 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 Authorised devices, software, and applications may be provided by Hawstead Parish Council for work-related tasks. Unauthorised installation of software on authorised devices, including personal software, is strictly prohibited due to security concerns.

10.2 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.

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

10.4 The Clerk shall arrange for regular review of the Council's website to ensure compliance with current legal requirements relating to website accessibility and shall ensure that an appropriate website accessibility statement is posted on the website.

11 EQUIPMENT SECURITY AND PASSWORDS

11.1 Councillors and officers are responsible for the security of (any) 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. Passwords should be strong and not shared with others. Regular password changes are encouraged to enhance security

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 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 our systems.

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 the Clerk immediately if they suspect a computer may have a virus and must report any email-related security incidents or breaches to the Clerk immediately.

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 Policy. 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.

16 SOCIAL MEDIA

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

16.2 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 our business in any way.

16.3 The Whatsapp protocol at appendix A shall be followed by all Members and the Clerk

17 PROHIBITED USE

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

17.2 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.

17.3 Any misuse of social media should be reported to the Clerk.

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 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 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 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 Council emails, files and data if there is a Council device available which can beused for that purpose.

20 RECORDS MANAGEMENT

20.1 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
Scales of fees and charges	6 years	Management
Receipt and payment account(s)	Indefinite	Archive
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
Quotations and tenders	6 years	Limitation Act 1980 (as amended)
Paid invoices	6 years	VAT
Paid cheques	6 years	Limitation Act 1980 (as amended)

VAT records	6 years generally but 20 years for VAT on rents	VAT
Petty cash, postage and telephone books	6 years	Tax, VAT, Limitation Act 1980 (as amended)
Timesheets	Last completed audit year 3 years	Audit (requirement) Personal injury (best practice)
Wages books	12 years	Superannuation
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.
Investments	Indefinite	Audit, Management
Title deeds, leases, agreements, contracts	Indefinite	Audit, Management
Members allowances register	6 years	Tax, Limitation Act 1980 (as amended)

Email correspondence need not be routinely retained for more than five years.

Appendix A Whats App Use protocol

Hawstead Parish Council is an elected body which makes decisions in duly convened public meetings. In between meetings, information is shared between members and the clerk by email correspondence. It is appreciated that from time to time members and clerk of Hawstead Parish Council need to share various pieces of information and news within the team speedily. With this in mind a dedicated Hawstead PC WhatsApp group has been established.

All members of the Council are welcome to join the group and we encourage you to join to receive the latest updates on scheduling of extraordinary meetings and any particularly urgent matter which needs to be brought to members' attention quickly.

The clerk will be responsible for the group as group admin and with your consent will add your phone number to the group. There is no obligation to use this channel of communication. Please be aware that the number you provide below will be visible and available to the rest of the group. You can opt to leave the group at any time and if you leave the Council's membership/employment your number will be automatically removed from the group.

WhatsApp Etiquette

Here are some tips to ensure everyone gets the most out of the Hawstead PC WhatsApp group:

- Understand that members of Hawstead PC give their time voluntarily; the clerk is employed for a few hours each week; it may not always be convenient or possible to respond within a particular timescale.

- Understand that Hawstead PC is a public authority and as such all communications on this group (and other mediums) are subject to Freedom of information Act 2000 and Data Protection legislation.

- Remember to be considerate and respectful to others

- Please be polite and observe the same level of courtesy as you would do if you were speaking to someone face to face

- Please refrain from commenting or sharing content (including videos or pictures) that could be interpreted as inappropriate, demeaning or inflammatory

- Please only discuss work related or business matters on the group and use alternative groups or chats for personal discussions

- Please do not share or discuss personal information of any residents or colleagues (this including names, contact numbers etc)

- Please do not share confidential information about any residents or individuals on the group

- Understand that the discussions will be moderated by the group admin and any inappropriate activity may lead to further investigation and potential action under the disciplinary procedure/ grievance procedure/ The Suffolk Code of Conduct.

If you have any queries or concerns about the group or its content please discuss this with clerk@hawstead-pc.gov.uk.