FLIXBOROUGH PARISH COUNCIL

The Village Hall
High Street
Flixborough
DN15 8RL

Clerk: 07716 183750
clerk@flixborough-pc.gov.uk
https://flixborough-pc.gov.uk

Email Account Policy

Date Policy Agreed	21st October 2026
Next Review	October 2028
Signature (Chair)	Sukai Wilkinson
Signature (Clerk)	Natasha Wilkinson

The email system is provided to allow electronic communication in carrying out Council business between Employees, individual Council service users and external organisations.

The Council owns the email facility, and emails that employees or elected members produce, send and receive are the property of Flixborough Parish Council.

Council Access to Email Accounts

The Council may access Councillor email accounts where necessary for legal compliance, FOI requests, data protection obligations, or continuity of business. Councillors must cooperate with any search for information required to fulfil a Freedom of Information request.

Professionalism and Integrity

- **Maintain Professionalism**: Parish Clerks and Councillors must use their gov.uk email addresses solely for official Parish Council business. All communications should be conducted with the highest level of professionalism and integrity. Councillors may send official emails where appropriate, but the Clerk remains the primary point of contact for external correspondence.
- **Respect Confidentiality**: Any sensitive or confidential information received via gov.uk email addresses must be handled with care, ensuring compliance with data protection laws.

Appropriate Use

- **Official Correspondence**: gov.uk email addresses should only be used for official correspondence related to Parish Council activities. Personal use or non-Council related activities are strictly prohibited.
- **Avoiding Misrepresentation**: Councillors and Clerks should not use their gov.uk email addresses to express personal views that may be misconstrued as official Parish Council positions.

Data Security

- **Password Protection**: Ensure that gov.uk email accounts are secured with strong, unique passwords and that these passwords are not shared. It is highly recommended to use Multi-factor Authentication for logging into your mail account.
- **Email Security**: Be vigilant against phishing, malware, and other cyber threats. Do not open attachments or click on links from unknown or suspicious sources. Emails that are identified as spam should be marked as spam and moved to the Junk/Spam folder. Any suspected data breach must be reported to the Clerk immediately.

Data Breach Reporting Requirement

- **Definition of a Data Breach** A data breach includes any incident where personal data is lost, accessed, disclosed, altered or destroyed without proper authorisation. This includes accidental sending of information to the wrong recipient, loss of a device, or unauthorised access to an email account.
- **Immediate Reporting** Any councillor or employee who becomes aware of a potential or actual data breach must report it to the Clerk **immediately** and without delay.
- **Clerk Responsibilities** Upon receiving a report, the Clerk will:
  - Assess the nature and severity of the breach
  - Take immediate steps to contain the incident
  - Determine whether the breach must be reported to the ICO
  - Record the breach in the Council's Data Breach Log
  - Notify affected individuals where required by law
- **Cooperation** Councillors and employees must cooperate fully with any investigation into a data breach and follow any instructions issued to mitigate further risk.

Record Keeping

- **Archiving Communications**: Parish Clerks must ensure that all official communications conducted via gov.uk email addresses are appropriately archived in accordance with legal and regulatory requirements. Local copies of emails or backups should not be held by Councillors.
- **Deletion of Email:**
  - Routine correspondence: retain 2 years
  - Financial records: retain 6 years
  - HR records: retain according to Document Retention Policy
- **Transparency**: Ensure that all relevant email communications are accessible for public records where appropriate, maintaining transparency in council operations.

Conduct During Disputes

- **Maintain Civility**: During any disputes or disagreements, all parties must communicate respectfully and avoid inflammatory language. The use of gov.uk email addresses to harass, bully, or intimidate others is strictly prohibited.
- **Conflict Resolution**: Seek to resolve conflicts through established council procedures rather than through email exchanges.

BYOD / Personal Device Security

- **Use of Personal Devices:** Councillors and Parish Council employees may access their gov.uk email accounts on personal devices (including mobile phones, tablets and home computers) only where those devices meet the security requirements set out below.
- **Minimum Security Requirements:** Personal devices used to access council email must:
  - Have a secure lock screen (PIN, password, fingerprint or facial recognition).
  - Have up-to-date operating system and security updates installed.
  - Have reputable anti-virus/anti-malware protection where applicable.
  - Not be shared with family members or other individuals when logged into council email.
  - Automatically lock after a short period of inactivity.
  - Not store council emails locally unless explicitly authorised.
- **Prohibition on Local Storage:** Councillors must not download, export or save council emails or attachments to personal device storage, cloud storage, or third-party applications. Access must remain within the approved gov.uk email environment.
- **Lost or Stolen Devices:** Any personal device used to access Council email that is lost, stolen or compromised must be reported to the Clerk immediately so that remote security actions (such as forced logout or password reset) can be taken.

Monitoring & Access

- **Council Ownership and Access Rights:** All gov.uk email accounts used for Parish Council business are the property of Flixborough Parish Council. The Council retains the right to access Councillor and employee email accounts where necessary to fulfil legal, regulatory or operational obligations.
- **Lawful Basis for Access:** Access may occur under the following lawful bases:
  - Compliance with the Freedom of Information Act 2000
  - Compliance with UK GDPR and Data Protection Act 2018
  - Continuity of business (e.g., councillor resignation, illness or vacancy)
  - Investigation of alleged misconduct or misuse
  - Retrieval of information required for statutory duties

- **Scope of Monitoring:** Monitoring will be:
  - Proportionate
  - Limited to what is necessary
  - Conducted only by authorised persons
  - Documented and carried out in accordance with data protection principles

The Council does not routinely monitor email content but may do so when required for the reasons listed above.

Compliance with Legislation

- **Adherence to Laws**: Parish Clerks and Councillors must comply with all relevant legislation, including the General Data Protection Regulation (GDPR) and the Freedom of Information Act, when using gov.uk email addresses.
- **Non-Discrimination**: All communications must adhere to equality and anti-discrimination laws, ensuring that no one is treated unfairly on the grounds of race, gender, disability, religion, or any other protected characteristic.

Reporting Misuse

- **Report Concerns**: Any misuse of gov.uk email addresses should be reported immediately to the relevant authority within the Parish Council or higher authorities as appropriate.
- **Investigations**: Reported incidents will be investigated promptly and impartially, with appropriate actions taken based on the findings.

Review and Amendments

- **Regular Reviews**: This Code of Conduct will be reviewed regularly to ensure it remains up to date with current laws and best practices.
- **Amendments**: Any amendments to this code must be approved by the Parish Council and communicated promptly to all parish Clerks and Councillors.

Acceptance of Terms

- **Agreement**: By using a gov.uk email address, parish Clerks and Councillors agree to adhere to this Code of Conduct and understand that any breach may result in disciplinary action.

Upon resignation or disqualification, councillor email accounts will be closed and all data retained by the Council.