Boughton Aluph & Eastwell Parish Council IT Policy

Adopted 11 February 2026

Introduction and background

Purpose and Scope

This policy applies to all councillors, staff, and other authorised users. It sets out the expectations for the appropriate use of IT equipment and systems provided by the council.

Email use protocols

- The council provides councillors & staff with email addresses @boughtonalupheastwellparishcouncil.gov.uk
- *Only* a parish council email address should be used for parish council business
- Parish council email must *only* be used for parish council business, not personal
- Users can download the Zoho email or files app, or log on via the Zoho website

Data Protection Responsibilities
- Staff, councillors and volunteers are responsible for keeping personal data secure and only Using it for the purpose it was collected for
- Contact the Clerk if a data breach has occurred, or you believe it may have occurred

Social Media
- Councillors and staff must be aware that they are responsible for anything that they write or present online. Care should be taken to distinguish where a view is personal, rather than a council position.
- Councillors should be mindful of the Members Code of Conduct and Nolan Principles
- Parish Council branded channels will be posted by the Clerk, in line with council policy and principally used as a virtual noticeboard with signposting towards the Parish Council owned gov.uk website as the most up to date source information

Use of council-owned devices
- Staff are provided with council owned devices to carry out their duties
- Council devices & software should be updated as updates are provided and replaced if they are no longer supported and will become insecure
- Staff should *only* use council devices to conduct council business

Zoho system & files
- The council provides a system to all councillors which includes individual and shared file storage areas, a virtual meeting system, office style software and email.
- Zoho enables councillors to not have to store data or documents on personal drives, councillors are encouraged to make use of Zoho files to enable them to not store documents on personal devices

Cyber security best practices
- Any devices used for parish council business should have up to date anti-virus software and updates should be installed as available
- Use strong passwords/PINs that cannot be guessed or use a password manager/generator. e.g.Last Pass
- Use 2 factor authentication on systems and devices where available
- Exercise caution opening attachments, particularly those that arrive unexpectedly

Leaving the council (councillors)
- Councillor email and Zoho accounts will be deleted when they leave the council
- Any physical or electronic data held should be deleted or returned (as appropriate)

Leaving the council (staff)
- Generic email accounts will be retained and enabled for continuity of access as they relate to the role (e.g. clerk@)

Training

Training is strongly recommended and available both online and in person:
Short online courses via KALC
Other courses from KALC including Data Protection for Councillors
(KALC & NALC courses can be booked via the Clerk)
Review

Further information is available from the
National Cyber Security Centre