MYNDTOWN COMBINED PARISH COUNCIL
Grouping Myndown, Norbury, Ratlinghope & Wentnor parishes

Assertion 10

Myndtown Combined Parish Council herein known as 'The Authority' recognises the importance of effective and secure information technology (IT) and email usage in supporting business, operations and communications as referenced by SAPPP, updated 2025 of The Practitioners Guide. Assertion 10 was introduced in April 2025 and is a separate mandatory requirement in the Annual Governance and Accountability Return (AGAR) for parish and town councils. It focuses on digital governance and data compliance, ensuring councils manage personal data responsibly, maintains secure IT systems and provides accessible online services.

Smaller Authorities IT Policy

This Policy outlines the guidelines and responsibilities for the appropriate use of IT resources and relevant data protection through email contact to and from the clerk, council members and any possible contractors or volunteers. In addition, this document confirms existing compliance with GDPR 2016, DPA 2018 for security and privacy, FOI 2000 and the Transparency Code for Smaller Authorities for document publishing.

1. Purpose & Scope.

This policy covers all member personnel using IT systems and resources for council business regardless of whether using council owned or their own personal devices. Should a member use personal devices they must use strong passwords for all accounts and use anti-virus software. Wi-Fi networks must be a trusted connection when carrying out official business. This Policy mainly applies to the existing Clerk who has been supplied with a Dell Laptop specifically for council business. The Clerk is responsible for maintaining digital security on the device and is the nominated DPO (Data Protection Officer).

2. Email Use Protocol.

The authority has an official generic role-based council email address parishclerk@myndtown.org.uk to provide a higher level of security. This is published on the authority owned domain http://www.myndtown.org.uk The email address is used for all correspondence on the council's own domain to risk losing access to records and violating GDPR if the clerk changes.

The Authority is in the process of considering permanent shared .org.uk email addresses for all council members by end of 2026 to minimise risk and GDPR control and prevent email forwarding to private accounts. However, this is not a Mandatory Requirement. Members must always check when sending confidential or sensitive information to the correct recipients. Caution is recommended when downloading or opening links to avoid phishing or malware and to verify links before clicking to open. All suspected security breach incidents must be reported immediately to the Clerk.

3. Website & Accessibility Compliance Statement.

The Authority website complies with WCGA2.2AA Standards:

- All Minutes, Agenda's, councillor information, AGAR's and other key documents are published on the domain to manage FOI, SAR & Transparency Code compliancy.
- The clerk is the only named individual data controller, data processor and DPO who manages the domain site. She is responsible for Risk Assessing all or any personal data before publication.
- There are no permanent staff (other than the clerk), contractors or volunteers therefore no personal data is stored on the domain site.

- Should a council member resign, their contact details will be deleted by the clerk and updated, when necessary, with a replacement member.
- Links to local community groups are published with their consent but no personal data is stored on the domain site.
- Regular audits for accessibility are scheduled yearly.

4. Data Protection Responsibilities

- No personal data is stored unencrypted on personal devices or cloud platforms without The Authority approval (GDPR Act 2018)

5. Use of Council Owned Devices

The Authority owns a Dell laptop installed with a secure accessibility password known only by the clerk and has the required anti-virus protections.

- The Authority laptop must not have software installed without prior consent.
- Should the existing clerk's role change, the laptop will be returned to The Authority with a hard copy of the password which can then be changed if necessary.
- Should tech support or issues arise, the clerk is responsible for seeking repair if necessary and will report at the next council meeting.

6. Cybersecurity Best Practises

The Authority laptop has anti-virus protection to prevent installing phishing & malware and is updated regularly.

- The clerk can recognise suspicious emails
- The password is unique to The Authority log-in
- The password is not shared across personal or social media communications i.e. Facebook
- The Authority has no official council social media page or platform other than the domain website.
- The Authority has no official WhatsApp group.
- The Authority members are discouraged from posting council activity on their personal social media platforms.
- For IT related enquiries or assistance, users can contact The Clerk parishclerk@myndtown.org.uk

Assertion 10: It is asserted that the procedures outlined herein have been implemented in accordance with all relevant standards and regulations. All The Authority members and the clerk are responsible for the safety and security of The Authority IT and email systems.

Signed: ..... Chair

Signed: …… Clerk

Date of Adoption: ……

Minute Ref: …….
Please Note a hard copy of this will be wet signed each year at The Annual Meeting in May.