



Cyber Essentials Working Group Terms of Reference

1 Remit

The working group is established to improve the efficiency and security of the IT systems that support the council's business. The group also aims to improve the IT skills and awareness of all Councillors and staff, and to increase understanding of and compliance with the IT Policy, first published in 2026. The group further aims to ensure that all IT systems provided by the Council comply with relevant government guidelines and standards. The longer-term objective of the group is to achieve formal certification for the Council under the government-run Cyber Essentials programme.

2 Frequency of meetings

The working group will meet four times a year, or more often if required.

3 Appointment of members

The working group will be appointed by the council and comprise at least three Councillors and at least one member of the Clerk team, with a quorum of two Councillors and one of the Clerk team.

The working group will appoint one Councillor member to chair meetings.

4 Delegated authority

The working group has no delegated financial authority.

The working group has the delegated authority to devise and deliver training material for the Council.

The working group has the delegated authority to configure security controls for all Council-owned IT systems, including software and hardware systems.

The working group has the delegated authority to assist the Clerk team to manage the Parish Council website to ensure it is secure, performs well, and complies with accessibility standards.

The working group has the delegated authority to complete the basic Cyber Essentials self-assessment questionnaire annually on behalf of the Council, and to submit it for external review.

5 Scope

The working group will present a written report of its activities to Full Council at least quarterly.

The working group may devise and deliver training sessions for Council staff & members to raise awareness of the provisions of the published IT Policy and to promote best practice in use of the email service and other systems provided by the Council.

The working group may make recommendations to Council for the purchase of any improved IT hardware or software that may be necessary to meet the Cyber Essentials standards

The working group should keep records of the security configuration of all systems being used for Council business – this should include hardware models and software levels in use, and it should include personally-owned devices being used by Councillors.

The working group may determine improvements to the security configuration of any IT systems provided by the Council, and work with the Clerk team to implement them.



The working group may make recommendations for improvements to the security configuration of personally-owned devices being used for Council business and may monitor and encourage compliance.

When the working group considers it appropriate, they may initiate the steps to achieve annual Cyber Essentials certification. These steps will include the following, repeated annually

- Review the current official HMG *Cyber Essentials Assessment* questions and the associated *Requirements for IT Infrastructure* document
- Draft the self-assessment answers using official online guidelines and resources
- Purchase an annual Cyber Essentials assessment (with prior approval from Council)
- Prepare and review the self-assessment answers online. At least two members of the working group, including one member of the Clerk team, must confirm the answers are accurate before final submission.

6 Review

Approved for use at the Council meeting on 8 June 2026. To be reviewed annually.

Signed:

Date: 8 June 2026

T E Thurston
Chair of the Council