Cyber Essentials for Key Stakeholders

Deciding to undertake a Cyber Essentials assessment is a positive step to reducing the school's risk of cyber-attack and demonstrating your school's dedication to cyber security.

Staff can sometimes feel anxious about the level of commitment and working time which may be required to achieve certification.

Cyber Essentials requires a whole school approach, and this document will highlight the role that each staff member can play in supporting the process.

Governing Board / Governor Representative

The governing board are ultimately responsible for the security and safety of the school.

A more detailed document will support the school in explaining to governors about Cyber Essentials requirement:

- Governors should promote the value of Cyber Essentials with staff.
- Recognise the additional staff time required to complete the assessment.
- Be prepared to review school security policies and procedures with reference to Cyber Essentials.
- Review the final submission and sign the submission declaration confirming the accuracy of the information supplied.

School Business Manager / School Business Officer

Cyber Essentials requires some generic school information which school office staff are well placed to answer. Whilst office staff are not responsible for the content of school policies, they are usually responsible for disseminating these to staff and have a good working knowledge of them.

It is likely that office staff can support in providing the following information:

- General school information, such as school name, address, and contact details.
- School budget confirmation (used to apply for the free cyber insurance).
- Access to school policies.
- Access to Acceptable Use Agreements (AUAs).
- Access to school inventories for hardware and software.
- Questions relating to the process of adding new users.

Headteacher

The headteacher will be ultimately responsible for agreeing the scope of the assessment. It is recommended that the whole school is included in order to maximise security and claim cyber insurance.

The headteacher will need to confirm how user access and administrative access is approved and documented.

In addition, the headteacher will need to confirm what actions are taken when it is believed systems are compromised.

Cyber Essentials for Key Stakeholders

IT Technician

The role of the IT Technician will vary, depending on whether they are employed as a member of staff, or whether support is outsourced.

It is likely that the IT Technician will have the appropriate knowledge of the school system to:

- Support in determining the scope of the assessment.
- Confirm changes to default passwords and detail how this is enforced for end users.
- Confirm whether routers and/or firewalls are accessible via the internet.
- Advise of the management of portable devices.
- Advise on malware protection, anti-virus software and updating protocols.

IT Providers

Whilst an IT Technician is on school sites regularly to support in practical tasks, it may be necessary to refer some queries to your providers if you outsource event management or utilise cloud services.

Wider staff and pupils

Each member of the school community plays a part in ensuring the safety and security of school systems.

Whilst wider staff and pupils will not be directly involved in the Cyber Essentials Assessment, their actions can support or prevent certification.

Ensure users are aware of and understand IT related policies and that the policies are readily available.

Ensure users have signed acceptable use agreements. It is likely that agreements for different types of user will apply.

Remind users to protect their user accounts by using strong passwords of at least 12 characters. If the account has the additional protection of multi-factor authentication (MFA), the password needs to be at least 8 characters long. Users need to ensure that their physical devices automatically lock when not in use, and need a biometric, password or PIN of at least 6 characters to gain access to the data and services available on that device.

Users should be advised of essential security precautions relating to the use of personal devices. This should include anti-malware protection.

Access to cloud services and remote network connection from home should be covered by policy which details minimum security expectations. MFA must be enabled on all accounts that access cloud services.

Users should change router default passwords and use a school VPN (virtual private network) if available.