Cyber Essentials Policy and Procedural Requirements

Remember that any policies or procedural changes will need to be reviewed and ratified by governors and a meeting minute number should be available.

IT Security Policy

1. Ensure your password policy is in place and meets the password based authentication requirements, as this is used in three of the five control themes.
2. Ensure the policy covers security updates (patch management) and malware prevention.
3. Ensure user access control is documented, including any authorisation process.
4. Include details of the process that should occur in the event that anyone feels a password is compromised.
5. Document the additional requirements for administrators including not using their elevated accounts for day-to-day tasks and the use of 2FA.
6. Detail the firewall requirements for the network boundary and for individual devices.
7. Include information about wireless devices, and document how access to guest Wi-Fi is authorised and provided.

Data Protection Policy

Remember that technical and organisational controls are essential as part of the Data Protection Act 2018 and UK GDPR.
Ensure that users are aware of when to utilise encryption or use a school VPN (Virtual Private Network).

Bring Your Own Device Policy

This policy should include the use of personal devices that connect to school networks, whether that be physical or cloud services eg Microsoft 365. In relation to apps, the policy is only concerned with those apps that interact with school data and services.
The policy should cover the following measures.

- Ensure that OS and apps are fully supported by the vendor.
- Ensure that software based firewalls are activated and configured correctly.
- Ensure all devices receive regular security updates, which includes updates for any apps.
- Ensure that Cyber Essentials password controls are applied to users own devices (BYODs).
- Ensure that users logging in, have a day-to-day account, and this is separate to the administrator account.
- Ensure that anti-malware software is installed on end user devices such as laptops, and a list of approved apps is provided for mobile devices.

Acceptable Use Agreement for users

An acceptable use policy should clearly outline expectations of what is acceptable and unacceptable behaviour when using school IT systems and equipment.

The agreement should be suitable for the end user and therefore, different agreements may be needed for different ages of pupils and for staff and visitors.
The agreement should include the stipulation that unapproved hardware devices and unapproved software will not be permitted.
You may need acceptable use agreements for the following:

- Pupils
- Staff
- Visitors / Supply Staff
- Governors
- System administrators

System administrator agreements should include the prevention of:

- Network traffic analysis tools or remote access tools to capture other users' data without consent.
- Services used to capture other users' network traffic and redirect their connections.
- Covert monitoring or data capture tools.

Offsite Working Procedure and Remote Learning Policy

If you are allowing users to connect remotely, ensure security requirements are explicitly referenced in any agreements and that the policies reflect behavioural expectations and security expectations, even in the home environment.

A procedure for new users and privileged users (administrators)

The process for provisioning new users should be clearly defined and understood. User access is a key part of Cyber Essentials certification.

Be sure that the process includes:

1. Providing staff with relevant policies.
2. Obtaining a signed Acceptable Use Agreement.
3. Understanding the minimum access level required to give access to necessary functions.
4. Approval for different access levels including a method to request access to the person who provisions the new account, and confirmation from the person who has provisioned the account as to what access has been granted.

Software and Hardware Inventories

Information audits already require schools to understand where personal data may be stored and these sit alongside the software inventory.

It is important that software is reviewed periodically to remove unnecessary applications.

Hardware inventories must be maintained as part of financial regulations, and write-offs should be authorised by governors and included in the minutes.

You should also have a Service Level Agreement (SLA) and contract with any third party IT supplier.