Cyber Essential – Five reasons for this accreditation

1. Compliance

The College is legally required to protect the data we hold within our organisation, particularly personal data of our students and staff. The introduction of The General Data Protection Regulation (GDPR), UK Data Protection Act in May 2018 means that the College must have solutions in place to protect that data and be able to demonstrate these.

Furthermore, the College must be able to show *why* this information is collected and have a plan to delete it when it's no longer needed.

2. Professionalism

Having Cyber Essentials certification demonstrates to students, suppliers and other partners that the College takes data security seriously and is proactively adhering to GDPR legislation.

Because Cyber Essentials is accredited by the government and used nationally, it's a quick way to show prospects that the College has done its due diligence and has systems in place to protect information. This gives them more confidence that they can trust the College and encourages them to work or study with us.

3. Increases in Cyber Attacks

Cyber-attacks are on the increase. Collages are a prime target and can have their systems wiped or find themselves locked out, have viruses installed or personal information stolen. Without robust cyber security solutions in place, your data is vulnerable to criminals.

4. Security

It's easy to think that because users are using passwords that Colege data is secure, but that's not always the case. Unfortunately, there is as much risk from attack due to human error (phishing email links) as there is from a concentrated outside cyber-attack. Staff often use their personal devices to access work systems or take their equipment offsite. Anyone can be fooled by 'man in the middle' email, where a cyber attacker impersonates the endpoints of an online information exchange to collect data (for example, pretending to be your bank or you to your bank to collect sensitive information).

It is important to use strong long passwords made up of many words (four is recommended) and include capitals, numbers and special characters. Currently College policy requires this be changed to a new unique password every 90 days.

5. Proactively Resolve Vulnerabilities

With staff and students able to access work information and the internet from a range of devices, the use of cloud storage and backup makes this more secure. By using a twostep verification process, this checks identity at login via a private mobile phone or email address

when accessing cloud systems. If credentials have been lost this will prevent a hacker from gaining access.

Cyber Essentials evaluates potential weaknesses in College systems and helps the organisation become stronger.