All Saints Schools Trust

Cyber Awareness Policy 2022-23

Authorised By:	ASST Board
Status:	Approved
Chair of ASST Board Signature	James Hargrave:
Date Approved:	February 2023
Next Review Date:	February 2024

Support in creating this policy is credited to: National Cyber Security Centre (NCSC), Cyber Essentials & JC CommTech

All Saints Schools Trust – Cyber Awareness Guidelines 2023-24

1. Rationale

ASST is aware of its legal obligation to keep personal data safe and that cyber security is a management and assurance issue, therefore it is important that everyone follows good basic principles. Cyber security is about protecting the devices we all use and the services we access online – both at home and work from theft, damage and the prevention of unauthorised access.

Schools hold a lot of sensitive data within several programmes (SEN, Behaviour, Assessment, Finance, Personnel records etc) and criminals appear to be currently targeting schools as they can be seen as an easy option'. Attacks can take many forms and information on the latest guidance please see:- NCSC Stay Safe Online - Top Tips

2. Aims

Staff will act with integrity and in the best interest of the schools within the Trust to ensure the risk of a cyber incident is kept to a minimal. Cyber incidents can seriously impact the Trust either by a phishing attempt to steal money and passwords, or by a ransomware attack that encrypts files preventing access.

This policy is aimed to increase awareness and convey the importance of following good cyber security guidelines and what to do if a cyber incident occurs.

It is important to consider the devices used within schools to ensure they are fully supported – this means that the device still receives regular security updates and is not in a vulnerable state. Any software stored on the device or used on-line should be assessed to ensure it fulfils an essential need and also noting which licences automatically renew on an annual basis. Any software programmes which are no longer required should be deleted with the aid of IT Support to ensure any personal data is removed.

As part of a Cyber Essentials assessment a register should be maintained of all devices/software used by individuals working at each school and confirmation is sought to ensure it is current and information is held securely by each school.

Confirmation from members of staff should be sought to ensure that devices owned by the Trust or individual schools should only be used for Trust or School business.

Similarly, Cyber Essentials suggests that a list is maintained of all devices owned by individuals who access School/Trust data either at home or school to seek assurances that these also receive security updates. Confirmation will be sought to ensure devices use authentication methods to avoid any inappropriate access.

Firewalls should be installed to on devices both a work and at home to ensure that any breaches are contained.

3. Application

The Headteacher of each school is responsible in ensuring that staff are aware of Cyber Security and that registers are maintained on the devices owned by the school, used or owned by staff at home and the software accessed on them.

Support in creating this policy is credited to: National Cyber Security Centre (NCSC), Cyber Essentials & JC CommTech

Staff should be encouraged to attend Cyber Security training, particularly those who access personal data. The National Cyber Security Centre provides a free online awareness course and can be found here: NCSC Free Online Training

4. Passwords

When implemented correctly, passwords are a free, easy and effective way of helping to prevent unauthorised users accessing devices or networks. Whilst passwords should be changed regularly, it is more important to ensure the quality of the password being used.

It is important to:-

- Use a different password for each account or service accessed.
- Passwords should be minimum of 12 characters using a mixture of upper/lower characters and signs.
- Three random words are suggested.
- Passwords must be easy to remember but hard for someone else to guess.
- If you must write it down, store securely away from your device.
- Do not leave your device unattended unless you lock the screen
- If a default password was provided – ensure this is changed as soon as possible.

The National Cyber Security Centre suggests that you DO NOT create a password which is any of the following:

- Partner's name
- Child's name
- Pet's name
- Place of birth
- Favourite holiday
- Something related to your favourite sports team
- A list of numbers (e.g. 123456) or words like 'password' or 'qwerty'.

Guidance on creating passwords can be found at: Password support

5. Phishing

A Phishing attack is where a scammer has sent a fake email pretending to be 'the real thing'. Staff need to be vigilant when opening ANY email as a virus could download when an attachment is opened.

Any member of staff who may have inadvertently opened an email purporting to be legitimate should report the incident to their Headteacher. An immediate response could reduce the severity of a cyber security incident.

6. USB / Pen Drives

We recommend that staff DO NOT use USBs or Pen Drives to save data as they will fail at some point and could spread viruses and malware from one computer or network to another.

Schools are asked to consider setting up a secure shared area or encourage staff to email the work to themselves.

7. Working from home

Support in creating this policy is credited to: National Cyber Security Centre (NCSC), Cyber Essentials & JC CommTech

With a lot of programmes accessible via the internet it is becoming increasingly easy to accomplish tasks from home instead of only conducting them in the work environment. Emails in particular can be accessed on a variety of devices. Care should be taken to ensure the internet is accessed through secure channels I.e. Home internet router or mobile phone mobile data and not hotspots. Firewalls should be installed on devices to increase security.

It is important to remember that staff are still responsible for keeping work information safe rven when accessing it from home.

To minimise cyber security incidents staff must:

- Ensure up-to-date anti-virus software is on your device.
- Only download apps through a recognised and reliable source I.e. Google Apps,
- Download and install all software updates as soon as they are offered.
- Ensure all your devices have passcodes and change any default passwords.
- Devices owned by the school should only be used for school business, thus limiting cyber security incident risk.

8. Trust Obligations

The Trust will fulfil their obligations by ensuring risk is minimised by unauthorised personnel to data held at Trust level.

Each school is responsible to ensure the integrity of all data held at school level.

Each member of staff should ONLY use Trust/School email address for Trust/school business purposes rather than personal ones.

The Trust will be seeking assurance from Executive Headteachers that all staff are aware of their responsibilities and have an awareness of Cyber Security and how to minimise risk .

The Trust will seeking assurances from Executive Headteachers that all staff are aware of their responsibility to ensure the integrity of all data and have an awareness of Cyber Security and how to minimise risk of unauthorised access.

9. Cyber Incident Management

In the event of a incident it is important for staff to report to their Headteacher immediately, who in turn should speak to the Trust Office. Headteachers should contact Action Fraud on 0300 123 2040 or go to www.actionfraud.police.uk to report the incident and gain support from your IT Support Service.

Action Fraud will provide technical advice and guidance, furthermore, in some circumstances they may deploy an incident response team to provide technical support.

The National Cyber Security Centre (NCSC) can access information to understand the incident better, identify the attacker, their likely motivations, if there are any other victims and if a compromise is likely to spread.

NCSC will co-ordinate any cross-government response, helping you to work with relevant government bodies, and ensuring public communications are aligned.

Support in creating this policy is credited to: National Cyber Security Centre (NCSC), Cyber Essentials & JC CommTech

Support in creating this policy is credited to: National Cyber Security Centre (NCSC), Cyber Essentials & JC CommTech