Cyber Security Policy

ODBST Level 2 Policy:	**ALL** Schools require this policy, **which may be adapted** where identified to suit local requirements and schools may add their own branding. LGBs will **note** adoption of this locally adapted policy in LGB meetings. Review will take place at Trust level, and schools will be notified of updates and review dates as necessary.
Other related ODBST policies and procedures:	Data Protection Policy E-Safety Policy CCTV Policy
Committee responsible:	FRAPP
Approved by:	FRAPP
Date Approved:	27th September 2023
Review Date:	Autumn term 2024

Cyber Security Policy

What is cyber security and why it matters to schools
Cyber security is about protecting the **devices** we use, and the **services** we access online from theft or damage. It is also about preventing unauthorised **access** to the vast amounts of personal data we store on these devices and in online accounts.

A cyber security incident can affect the school's ability to function, the security of its data, its reputation and finances. The implications for schools that are successfully targeted are both significant and costly. Examples of the impact may include:

1. Informing the Information Commissioners Office that sensitive information has been lost.
2. Managing the communication of a data breach with pupils, staff, partners, and parents.
3. Losing all the schools' systems for an unknown time period.
4. Commissioning IT expertise.
5. Significant reputational damage
6. Creating safeguarding risks for children and young people.

Both the school leaders and the governing body will want to ensure they are aware of cyber risks and adequately prepared in the event of a cyber incident.

Roles and responsibilities
The role of local governing board is strategic and should be focused on ensuring that the school has IT policies and procedures in place that cover the use of ICT systems and data security, including compliance with the General Data Protection Regulations (GDPR).

To Ensure cyber security XXXXX School will carry out the following action linked to three themes:
to **seek out information**, **raise awareness**, and **improve preparedness** in case of a cyber incident.

Theme A: Information Seeking

- Keep a list of all organisations that provide the school's IT services. Eg who provides the school's internet connection; runs the school's website; IT support contracts from a Local Authority or a Managed Service Provider. These should all be on the Information Asset Register (stored in Safesmart Smartlog).

- Have a school IT coordinator or manager and that this person/team/company follows key cyber security practices as outlined in the RPA Cyber Security requirements.

- Ensure the school complies with the Risk Protection Arrangements (RPA) cover requirements for Cyber Cover as listed below:

RPA members must comply with the following conditions for cover to apply. In the event of a claim the Member will be required to evidence compliance with all of the conditions below:

- All members must have 3 offline backups: The Department for Education InfoSec Team provides the following guidance to schools: It is vital that all education providers take the necessary steps to protect their networks from cyber-attacks and have the ability to restore systems and recover data from backups. Education providers should ensure that IT teams are:

i. Backing up the right data. Ensuring the right data is backed up is paramount, including but not limited to; Covid-19 information, data relating to exams/coursework, student/staff data and alongside other key elements.

ii. The backups are held fully offline and not connected to systems or in cold storage, ideally following the 3-2-1 rule explained in the NCSC blog Offline backups in an online world: https://www.ncsc.gov.uk/blogpost/offline-backups-in-an-online-world

iii. Backups are tested appropriately, not only should backups be done regularly but need to be tested to ensure that services can be restored and data recovered from backups.

Further Help and guidance can also be found on: Step 1 - Backing up your data - NCSC.GOV.UK. https://www.ncsc.gov.uk/collection/small-business-guide/backing-your-dataportal.

All ODBST schools must have a Cyber Response plan. The DFE provide one for schools to use: RPA-Cyber-Response-Plan-Template-V1.0.pdf (rpaclaimforms.co.uk)

Theme B Raise Awareness

School's governance and IT policies must reflect the importance of good cyber security.

Cyber incidents or attacks should be considered in terms of risk management and be listed on the school's risk register, alongside other IT and data risks. Cyber security should be referenced in all relevant school policies (e.g. business continuity, data protection, acceptable usage etc). ODBST advises that cyber security is a regular agenda item at governing body meetings as with other topics like GDPR and the physical security of the school.

All ODBST schools must train staff and governors about the common cyber security threats and incidents that schools experience. Good cyber security is dependent on people. Staff can alert schools to potential problems like spotting phishing emails or phone calls, or noticing when a service is running particularly slowly, which could be a sign of a cyber-attack.

Free training can be accessed through the NCSC's website or through Safesmart Smartlog. There are other training resources like the Practical Tips guide which can be downloaded from the NCSC's website or on The Key. The Key's staff briefing can be found in Safesmart Cyber security folder. This includes question and assessment ot ensure staff have a solid understanding and impact of this training can be proven

Theme C: Preparedness

Being prepared for the potential impact of a cyber security incident is crucial in helping schools minimise disruption should an incident occur.

All ODBST schools have a Business Continuity Plan to prepare for temporary loss of access to its data and/or internet connection to support it staying open in the event of an incident.

A cyber incident could result in a school's network being unavailable for an unknown period of time, with limited or no access to important data and services. The importance of access to the MIS has been covered earlier in theme A, but there are other services like: telephones, access control systems, cashless payment systems. These will impact on the school's operation if they are unavailable.

The school's Business Continuity Plan will identify what they will do such as for example, implement suitable defences, focused on mitigating risk, holding paper copies of the school register and parent contact information. This way a school can increase its chances of functioning in the event of a cyber incident. Key to this is the list of IT service suppliers the school uses including contact numbers. Schools should refer to their Cyber Response Plan in the event of an attack.

In the event of a cyber security attack

- Do not click on any link that the ransomware provides for you.
- Switch everything off.
- Contact your IT support.
- Refer to the contact list in their Business Continuity Plan which will identify the relevant people and support, external IT supplier/providers as well as those responsible for the management of IT within the school. This contact information and plan must be kept up-to-date and reviewed regularly.

Next steps

- Inform the **National Cyber Security Centre** - Reporting a cyber security incident (ncsc.gov.uk)
- Inform **CEO** and **Chief Operations Officer**- **079391 416990**, leave contact details and summary of situation
- Inform the **ICO if there is a data breach** - Report a breach | ICO
- Inform the **police** via Action Fraud
- Inform the Chair of the governing body.

TERM	DEFINITION
Antivirus	Software designed to detect, stop and remove malicious software and viruses
Breach	When data, systems or networks are accessed or changed in a non-authorised way
Cloud	Where you can store and access your resources (including data and software) via the internet, instead of locally on physical devices
Cyber attack	An attempt to access, damage or disrupt your computer system, network or devices maliciously
Cyber incident	Where the security of your system or service has been breached
Cyber security	The protection of your devices, services and networks (and the information they contain) from theft or damage
Download attack	Where malicious software or a virus is downloaded unintentionally onto a device without the user's knowledge or consent
Firewall	Hardware or software that uses a set of rules to constrain network traffic – this is to prevent unauthorised access to or from a network
Hacker	Someone who uses their computer skills to break into computers, systems and networks
Malware	Malicious software including viruses, trojans or any code or content that can adversely impact individuals or organisations
Patching	Updating firmware or software to improve security and/or enhance functionality
Pentest	Short for penetration test. An authorised computer network or system test to look for security weaknesses
Pharming	An attack on your computer network where users are redirected to the wrong website even if they type in the right website address
Phishing	Untargeted, mass emails sent to many people asking for sensitive information (like bank details) or encouraging them to visit a fake website
Ransomware	Malicious software that stops you from using your data or systems until you make a payment