*E-Security Policy

White Spire School

Approved by:	Michelle Bartle	**Review Date:**	22/05/2024
Next review due	22.05.26		

Commented [SS1]:

Strategic and operational practices

At this school:

- Finlay Douglas is the Senior Information Risk Officer (SIRO).
- Matt Regan is the Data Protection Officer (DPO) with responsibility for data protection compliance.
- Staff are clear who the key contact(s) for key school information are (the Information Asset Owners). We have listed the information and information asset owners in the Schools Information Asset Register.
- We ensure staff know to immediately report and who to report to, any incidents where data protection may have been compromised, such as when passwords for sensitive systems or devices are lost or stolen, so that relevant action(s) can be taken.
- All staff are DBS checked and records are held in the single central record.
- We have approved educational web filtering across our wired and wireless networks. Pupil activity is filtered and monitored using the Securly platform and staff activity is monitored and filtered using the Opendium Web Gateway.
- Our web filtering services are checked termly by both the IT Manager and the deputy head/DSL. These checks are signed and logged.
- We also have additional layers of monitoring across our networked systems.
- We monitor school e-mails / blogs / online platforms / social media / web searches / web traffic, to ensure compliance with the Acceptable Use Agreement. As well as monitoring usage, we may also monitor content of these streams.
- We follow Local Authority guidelines for the transfer of any data, such as MIS data or reports of children, to professionals working in the Local Authority or their partners in Children's Services / Family Services, Health, Welfare and Social Services.
- All staff have their own unique username and private passwords to access school systems. Staff are responsible for keeping their passwords private.
- We require staff to use strong passwords for access into our MIS systems and cloud storage.
- We require that any personal/sensitive material must be encrypted if the material is to be removed from the school, and limit such data removal. We have an approved cloud storage platform so staff can access sensitive and other data from home, without need to take data home.
- School staff who set up usernames and passwords for e-mail, network access and other online services work within the approved system and follow the security processes required by those systems.
- We ask staff to undertake housekeeping checks at least annually to review, remove and destroy any digital materials and documents that need no longer be stored.

Technical or manual solutions

· We require staff to either log-out or screen-lock systems when leaving their computer.

· Staff have secure areas on the network to store sensitive documents or sensitive photographs.

· We use DO NOT use email to send attached documents outside the school except known LA units.

· We use encrypted flash drives/encrypted tablets if staff have to take sensitive information off site.

· We use the SIMS to securely transfer pupil data to/from other schools.

· We use Egress Switch to securely transfer files to other institutions.

· We use Google Drive for cloud document storage. No other cloud storage is permitted.

· We use 2-factor authentication for remote access to sensitive data in cloud storage

· We store any sensitive/special category written material in lockable cabinets in a lockable area.

- All servers located are in locked rooms or cabinets and managed by DBS-checked staff.
- We use 2-factor authentication for remote access into our systems and only permit remote access when deemed absolutely necessary.
- Onsite back-ups are stored in locked and secured cabinets/rooms. No back-ups leave the site on mobile devices.
- Off site back-ups are encrypted.
- We use RedStor / MS Backup / Duplicati for disaster recovery on our Windows servers.
- We also use Xen image management for disaster recovery on all our servers.

- We comply with the WEEE directive on equipment disposal, by using an approved disposal company for disposal of IT equipment. For systems (such as servers, printers, etc), where any protected or restricted data has been held, the storage devices are securely wiped (or the storage device is removed and physically destroyed if secure wiping is not possible).
- Portable equipment loaned by the school (for use by staff at home), where used for any protected data, is disposed of through the same procedure.
- Paper based sensitive information is disposed of by shredding, using a crosscut shredder.