E-Security Policy

MISSION STATEMENT.

Together with Jesus, we will Love, Learn and Grow in Faith

Strategic and operational practices

At this school:

- The Head Teacher is the Senior Information Risk Officer (SIRO).
- Mr Strom is the main point of contact for data protection in school. The Data Protection Officer (DPO) with responsibility for data protection compliance is a statutory role that is fulfilled by Angela Lewis through our SLA.
- 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 a spreadsheet, located on the admin shared drive.
- 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 one central record – located on the admin confidential shared drive. We ensure ALL the following school stakeholders sign an Acceptable Use Agreement. We have a system so we know who has signed.

  - staff
  - governors
  - pupils
  - parents
  - volunteers

  This makes clear all responsibilities and expectations with regard to data security.

- We have approved educational web filtering across our wired and wireless networks. We monitor school e-mails / blogs / online platforms, etc. to ensure compliance with

the Acceptable Use Agreement. As well as monitoring usage, we may also monitor content of e-mails / blogs / etc.

- We follow LA guidelines for the transfer of any data, such as SIMS 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 SIM system.
- We require staff to change their passwords into the MIS, USO admin site, other secure system every 90 days / twice a year.
- 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 remote access solution 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 house-keeping checks at least annually to review, remove and destroy any digital materials and documents which need no longer be stored.

Technical or manual solutions

- Staff have secure area(s) on the network to store sensitive documents or photographs.
- We require staff to log-out of systems when leaving their computer, but also enforce lock-out after 10 minutes idle time.
- We use encrypted flash drives if any member of staff has to take any sensitive information off site.
- We use the DfE S2S site to securely transfer CTF pupil data files to DfE / other schools.
- We use G-Suite for Education for online document storage.
- We store any sensitive/special category written material in lockable storage cabinets in a lockable storage area.
- All servers are in lockable locations and managed by DBS-checked staff.
- We use Micro-soft Azure online Backup for disaster recovery on our <network / admin, curriculum server(s).
- We comply with the WEEE directive on equipment disposal, by using an approved disposal company for disposal of IT equipment. For systems, where any protected or restricted data has been held, (such as servers, photocopiers), we get a certificate of secure deletion.
- 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 shredded, using a cross-cut shredder.

Date of next review: October 2019

This policy is reviewed by: SLT / School technical support