


E-Security Policy

 Sutton House Academy	Name of Academy	Sutton House Academy
	Policy review date	June 2020
	Date of next review	June 2021
	Who reviewed this policy?	Board

Strategic and operational practices

At this Academy:

- The Headteacher is the Senior Information Risk Officer (SIRO).
- Karen Phillips is the Data Protection Officer (DPO) with responsibility for data protection compliance.
- Staff are clear who the key contact(s) for key Academy information are (the Information Asset Owners). We have listed the information and information asset owners in a spreadsheet or system
- 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.

We ensure ALL the following Academy stakeholders sign an Acceptable Use Agreement. We have a system so we know who has signed.

- staff
- governors
- pupils
- parents and carers
- 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 Academy 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 Academy 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 Academy systems. Staff are responsible for keeping their passwords private.
- We require staff to use STRONG passwords for access into our MIS system.
- We require that any personal/sensitive material must be encrypted if the material is to be removed from the Academy, 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.

- Academy staff who set up usernames and passwords for e-mail, network access, 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.
- When a member of staff leaves, on their last day of employment their emails system is frozen and they cease to have access to their emails and the shared area of the server; and that where a member of staff is off work for an indefinite period of time, incoming emails will be redirected to their line manager.

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 5 mins. idle time.
- We use RAV3 and a secure remote access server with its 2-factor authentication for remote access into our systems.
- We use the DfE S2S site to securely transfer CTF pupil data files to DfE / other schools.
- We use LGfL AutoUpdate for creation of online user accounts for access to services and online resources.
- We use LGfL's USO-FX2 to transfer documents to schools in London, such as references, reports of children.
- We use Google Drive & One Drive to store online documents
- 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 LGfL's GridStore remote secure back-up solution for disaster recovery on our servers.
- 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 Academy (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.