Electronic Security Policy

Strategic and operational practices

At this school:

- The Head Teacher is the Senior Information Risk Officer (SIRO).
- Danny Ward is the Chief Privacy Officer (DPO) with responsibility for data protection compliance and is the main contact person for compliance and liaison with the Information Commissioner's Office.
- Staff members are clear who the key contact(s) for key school information are (the Information Asset Owners).
- Staff members 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. A Data Breach form will be filled in by the most relevant person. Police will also be contacted where there is evidence of foul play or deliberate criminality.
- All staff members are DBS checked and records are held in one central record. 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 also have SOPHOS an additional layer of monitoring and security software across our network system.
  We monitor school online activity 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 LB Croydon 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 and ensure the use of Egress secure email or USO-FX2.
- All staff have their own unique username and private passwords to access school systems. Staff members are responsible for keeping their passwords private.
- Staff are automatically issued with strong passwords for access into the SIMS MIS system.
- We require staff to change their passwords into the MIS, USO admin site, every 90 days.
- 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 members who set up usernames and passwords for e-mail, network access, 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. This is addition to retention and disposal obligations under GDPR/Data Protection Bill 2018.

Technical or manual solutions

- Relevant Staff have secure areas 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 40 mins. idle time.
- We use encrypted flash drives if any member of staff has to take any sensitive information off site.
- We use RAv3/VPN solution 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 the Pan-London Admissions system to transfer admissions data.
- 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 LGfL's myDrive 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 LGfL's GridStore remote secure back-up for disaster recovery on our network admin and curriculum 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 school (for use by staff at home), where used for any protected data, is disposed of through the same procedure.
- Hard Drives are returned to us for destruction by ICADigital who have the contract to supply and maintain the bulk of our printers. These are inaccessible without administrator password access.