




## E - Security Policy

Governing Board with Responsibility	Full Governing Board	
Reviewed/Revised	Autumn 2022	
Date of Next Review	Autumn 2024	
Agreed by Governors	24.11.2022	
Additional Notes	This policy should be reviewed every 2 years or before if requested by the Governing Board or Headteacher.	

**When drafting and agreeing policy, governors always act with our four values in mind and our school vision as drivers for change or important decisions. We will ensure that: Policies positively impact on our staff and children’s growth, their faith, our unity as a school community and promote kindness as a thread through all we do. We act in line with our collective responsibility around equality and the protected characteristics and always make decisions that foster an understanding and respect for these.**

### Vision statement

**‘Belonging, learning and growth for life in all its fullness’**

### Mission Statement

At Princess Frederica we:

**Promote social, emotional, spiritual and educational growth in all our children**

*(This is how we develop character)*

**Impart the gifts of self-confidence, determination and curiosity with a rich and creative curriculum**

*(This is the way we educate)*

**Create a positive impact on our local and global community and environment**

*(This is our footprint on the world and community)*

**Nurture friendship, kindness and respect**

*(This is how we treat each other)*



## Strategic and operational practices

At this school:

- The Head of School is the Senior Information Risk Officer (SIRO).
- LDBS service is the Data Protection Officer (DPO) with responsibility for data protection compliance.
- 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 SCR.
- 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
  - volunteersThis 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 an additional layer of monitoring software across our network system (Sophos). We monitor school e-mails to ensure compliance with the Acceptable Use Agreement. As well as monitoring usage, we may also monitor content of e-mails.
- We follow LDBS 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 system.
- We require staff to change their passwords into the SIMS, e mail or other secure system 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 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.



## 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 mins.
- We DO NOT USE FLASH DRIVES OR HARD DRIVES.
- 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. Staff with access to the Admissions system also use a LGfL OTP tag as an extra precaution.
- 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 my Drive and shared Google drive for online document storage.
- We store any sensitive/special category written material in storage cabinets in a lockable storage area.
- All servers are in lockable locations and managed by DBS-checked staff.
- Back-ups are encrypted. No back-up tapes leave the site on mobile devices.
- We use LGfL' Grid Store remote secure back-up named alternative solution (redstone – GDPR compliant) 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 or disposed securely by using an approved company.