Rise Park Academy Trust	**Name of School**	**Rise Park Academy Trust Rise Park Infant & Junior Schools**
	Policy review Date	**20.9.2018**
	Date of next Review	**20.9.2019**
	Who reviewed this policy?	**Mrs L Nortje – Online Safety & Computing Lead & SLT**

Online Security policy

Strategic and operational practices

At this school:

- The Head Teacher is the Senior Information Risk Officer (SIRO).
- Staff are clear who are the key contact(s) for key school information (the Information Asset Owners) are.
- We ensure all staff know who to report any incidents where data protection may have been compromised – Carolyn Fox, Executive Head Teacher.
- All staff are DBS checked and records are held in one central record: SIMS, We ensure ALL the following school stakeholders sign an Acceptable Use Agreement form. We have a system so we know who has signed.
  - staff,
  - governors,
  - pupils
  - parents

  This makes clear staffs' responsibilities with regard to data security, passwords and access.
- We follow LA 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 password private.
- We require staff to use STRONG passwords for access into our system.
- We require staff to change their passwords into the MIS, USO admin site, twice a year.
- We require that any Protect and Restricted 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 – (Teachers will receive a Kingston USB stick which will be password protected and Portico will soon be available for access by all staff).
- School staff with access to setting-up usernames and passwords for email, network access and Learning Platform access are working within the approved system and follow the security processes required by those systems.
- We ask staff to undertaken at least annual house-keeping to review, remove and destroy any digital materials and documents which need no longer be stored.

Technical or manual solutions

- Staff have a secure area on the network to store sensitive documents or photographs (Fronter/RM Shared Server).
- We require staff to log-out of systems when leaving their computer.
- We will use encrypted USB sticks (once provided) until Portico is up and running 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 other schools.
- We use the Pan-London Admissions system (based on USO FX) to transfer admissions
- We use LGfL's USO FX to transfer other data to schools in London, such as references, reports of children.
- We use the LGfL secure data transfer system, Atomwide's AutoUpdate, for creation of online user accounts for access to broadband services and the London MLE,
- We store any Protected and Restricted written material in an area that is only accessible to adults (Fronter/RM Shared server).
- All servers are in lockable locations – dedicated server room and is managed by the ECC.
- We comply with <the WEEE directive on equipment disposal> by using an approved or recommended disposal company for disposal of system hard drives where any protected or restricted data has been held.
- 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 cross cut shredder.
- We are using secure file deletion software.