E-Security Policy

	Name of school	**Our Lady and St John's RC Primary**
	Policy review date	**Summer 2022**
	Date of next review	**Summer 2024**
	Who reviewed this policy	**Governors**

- This is a generic policy from LGfL who are our service provider.

Strategic and operational practices

At this school:

- ***Mrs Sue Cunningham, Head teacher*** is the Senior Information Risk Officer (SIRO).
- ***Mr Gary Padbury*** is the Data Protection Officer (DPO) with responsibility for data protection compliance.
- 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 or system – an Excel template is available at ***gdpr.lgfl.net***.
- We ensure staff know to report immediately 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 spreadsheet.(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
  - 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 an additional layer of monitoring software across our network system. 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 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 have an approved remote access system so staff can access sensitive and other data from home, without the need to take data home.
- School 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.

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.
- 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 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 Gigasoft remote secure back-up; and 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.