Data Security Policy

Your school logo	**Name of school**	**St John Bosco College**
	Policy review date	**17 May 2018**
	Date of next review	**May 2019**
	Who reviewed this policy	**School Business Manager**

Strategic and operational practices

At this school:

- The Head Teacher is the Senior Information Risk Officer (SIRO).
- James Smith 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 located within GDPRis Portal.
- 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 on SIMS.
- 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, network and online platforms, to ensure compliance with the Acceptable Use Agreement. As well as monitoring usage, we may also monitor content of e-mails.
- Data Protection breach records are located within the GDPRis Portal.
- 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 require staff to use STRONG passwords for access into our MIS system.
- We require staff to change their passwords into the MIS, network (single sign on) USO admin site, twice a year.

- 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 and 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 50 mins. idle time.
- We use encrypted flash drives if any member of staff has to take any sensitive information off site.
- We use VMware Horizon solution for remote access into our systems.
- We use the DfE S2S site to securely transfer CTF pupil data files to DfE / other schools.
- All staff *and* governors use office365 staffmail for all school related email.
- We use encrypted emails or S2S to transfer documents to schools in London, such as references, reports of children.
- We use office 365 onedrive 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.
- Back-ups are encrypted.
- We use LGfL's GridStore remote secure back-up for disaster recovery on our admin and 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.

- Appendix - Subject Access Request Form
- Appendix - Data Breach Procedure
- Appendix – Roles & responsibilities of the Data Protection Officer
- Appendix – Privacy Impact Assessment record