All Saints Catholic High School
Data Protection and GDPR Acceptable Use Policy – School Workforce (including Supply Staff, ITT Students and Governors)

The use of data has an important role in the running of the school and it underpins the teaching and learning process. At All Saints Catholic High School we acknowledge that using data has great benefits and that it is important to balance those benefits with an awareness of the potential risks of using, sharing and transferring the data. The school is committed to safeguarding and the well-being of our students and staff.

We expect that the school workforce will;

- take responsibility for ensuring their passwords to access the network services including email are at least 7 characters in length and follow the guidance in the school handbook for internet security *(guidance under review)*
- take responsibility for their own conduct in the responsible use of data in school and outside of school, this includes not sharing with other parties*
- following the email protocols, particularly for those emails that may contain personal data *(protocols under review)*
- understand that if they send emails relating to work that they do so in a responsible and professional manner ensuring that sensitive data cannot be shared with third parties.
- maintain a 'clean screen' data environment in the classroom or work area and take responsibility to ensure that other sensitive data is not visible to students e.g. SIMS is not displayed/ accessible to students and other students data is not visible at parents evenings etc.
- understand that they are responsible to report a data breach to the Data Protection Officer (DPO) Mr J Prosser immediately
- understand that that files containing personal data should be stored appropriately e.g. in secure network areas or in locked filing cabinets
- ensure that staff who use personal devices to access personal student data have secure passwords and have adopted a practice that means third parties cannot access this data e.g. shared devices at home
- understand memory sticks must not contain personal data
- refer any requests for personal data (Subject Access Requests) made by a parent or student directly to the DPO
- ensure that any images, still or video, of students are taken with their consent, taken on school devices, uploaded to the network drives or social media feeds and then deleted from the camera or its memory card
- ensure that events that require personal data to be used have been approved by the DPO for GDPR compliance e.g. school trips

* exceptions are those staff who share data which is in the public interest or for the legitimate needs of running the school who are recognised by the School as part of the data processors group. This may include but is not limited to:

- SIMS;
- Safeguarding;
- Exams;
- Admissions

These staff must ensure they use secure file transfers to other agencies using Anycomms or by means of password encrypted files.

You can view the full GDPR policy and privacy notices on the staff virtual learning environment (VLE)