Acceptable use policy for IT, including school systems, email, personal devices, messenger applications and social media

St Olave's 8–13 YORK

Please read through both pages of this document, sign and return one copy and retain a copy for your information

Digital technology plays a significant role in the lives of young people, and the school recognises its importance in education. The school provides access to resources such as the Internet, computers, software, storage, printing facilities and other equipment to support teaching and learning. Our expectations for pupil behaviour online are an extension of those for all other aspects of life at St Peter's. Pupil use of IT and digital technology must always be within the law, and respectful of the values of the School.

School-provided WIFI, email, software applications and cloud-based storage

All pupils have access to the Internet at St Peter's via school devices. Pupils also have access to school-provided email accounts, software applications and cloud-based storage, accessible via their own, or School-provided, devices. Any use of School devices, systems or applications to access, generate, store or share material that is obscene, politically extreme, defamatory or otherwise offensive may attract formal sanctions, and may also be illegal. In order to protect users from illegal content and malicious or harmful communications, the School applies filters to its internet link, access to which is monitored.

Pupils' use of the Internet via their own devices and use of mobile phones

Whenever a pupil is on-site, or off-site on a school activity, the same rules apply to usage of the internet, including messenger services and social media, when accessed via a personal device and data plan, as would apply if the same services were accessed using a school-provided device, or the school network and WIFI.

During class time pupil mobile phones should not be used or be visible unless this is specifically authorised by the teacher as part of learning. Mobile phones should also not be used during the school day without the express permission of a member of staff, for a specific reason.

Cyberbullying

Bullying, harassment, intimidation or exclusion of others using online platforms, email, social media applications or messenger services is regarded as a serious breach of discipline, regardless of whether this occurs on or off the School premises, in term-time or during the holidays, and may result in a formal sanction.

User-generated sexual images (sexting)

The generation and sharing of naked or sexual images of a child (including by themselves) is illegal, a breach of safeguarding, and may constitute a serious criminal offence relating to child pornography, grooming and peer-on-peer abuse. In such cases the School may be required to share any such images with the Police, in line with its legal duties.

Security and safety

Staff may review pupil files and communications conducted on the school network to ensure that usage is appropriate and lawful. The school supports the safe cloud-storage of pupil files through pupil access to Office 365 and its applications. It also maintains firewalls and other protective systems to prevent harm to users and their files.

Pupil-owned devices

As stated in the School's Behaviour and Discipline Policy, a pupil-owned device may be confiscated and searched if there is reason to believe that that data or files have been used to cause harm, to disrupt teaching, or to break School rules. If inappropriate material is found on a pupil-owned device, a Staff member may delete the material, retain it as evidence of a breach of School discipline or criminal offence, or hand it over to the police if the material found is of sufficient seriousness to warrant this.

Summary

In order to:

- Uphold all relevant laws, safeguarding duties and the School's values
- And promote the safe and effective use of digital technology

Pupils must not:

- Use school-provided internet access, devices, storage or software applications for the generation, storage, sharing or display of material that is obscene, politically extreme, defamatory or otherwise offensive, or to commit any criminal activity of any type.
- Use any device, software application or platform to harass, bully, intimidate or exclude any other pupil, whether using School-provided or personal devices, whether on site or off site, during term time or holidays.
- Generate or share any sexualised or unclothed imagery of themselves or another pupil, including taking images inside the clothing of another pupil.
- Bring the School into disrepute through the publication or sharing of obscene, politically extreme, defamatory or otherwise offensive material via social media or other online platforms.
- Engage in behaviour harmful to the school network, systems and devices, including through the downloading of viruses, malware or other harmful programmes, or by circumventing security and monitoring systems designed to protect all users.
- Unlawfully access data systems, or the profiles, email accounts or files of other users.
- Use mobile phones in those circumstances prohibited by this acceptable use policy.

Acceptance of guidelines:

On joining the School, all pupils must adhere to the agreement regarding the proper use of devices (both School-provided and personally owned), WIFI, cloud storage and software applications, when in School or engaged in School activities when off-site. Signing this agreement also constitutes your agreement that the school will monitor your child's use of IT when you are logged into the School system.

Updated June 2020