



St. Francis' College ***Safe Use of Mobile Technology Policy (Pupil)***

Introduction

The 'College' refers to all the staff and pupils of the Prep Department and Senior School which includes Early Years Foundation stage (EYFS), Pre-Prep (Key Stage 1), Prep (Key Stage 2), and Senior School (Key Stages 3-5).

The Role of Technology in Our Pupils' Lives

Technology plays an enormously important part in the lives of all young people. Sophisticated games consoles and mobile phones provide unlimited access to the internet, to SMS messages, to blogging services (like Twitter[®]), to Skype[®] (video calls, via web cameras built into computers, phones and PSPs), to wikis (collaborative web pages), chat rooms, social networking sites. This communications revolution gives young people unrivalled opportunities. It also brings risks. It is an important part of our role at St Francis' College to teach pupils how to stay safe in this environment and how to avoid making themselves vulnerable to a range of risks, including identity theft, bullying, harassment, grooming, stalking and abuse. They also need to learn how to avoid the risk of exposing themselves to subsequent embarrassment and exploitation. In agreement with KCSIE 2021, we recognise that 4G and 5G data access can pose additional safeguarding dangers such as accessing restricted material and engaging in online peer-on-peer abuse.

The Role of ICT Staff

The College technical staff have a key role in maintaining a safe technical infrastructure at the College and in endeavouring to keep abreast of the rapid succession of technical developments. They are responsible for the security of our hardware system, our data. The e-safety Co-ordinator is responsible for training our teaching and administrative staff in the use of ICT. They monitor the use of the internet and emails and will report inappropriate usage. With the explosion in technology, we recognise that blocking and barring sites is no longer adequate. We need to teach all of our pupils to understand why they need to behave responsibly if they are to protect themselves. This aspect is a role for all staff using ICT with pupils, but particularly the College's Designated Safeguarding Lead, who is responsible for e-safety and our pastoral staff.

Role of our Designated Safeguarding Lead

St Francis' College recognises that internet safety is a child protection and general safeguarding issue. The Deputy Head, who is the Designated Safeguarding Lead and also our e-Safety Officer, works closely with the ICT staff and Head of ICT. All teaching staff have been trained in the safety issues involved

with the misuse of the internet and of mobile devices and safety education is part of ICT lessons and the PSHE educational programme. It is the responsibility of the DSL to handle allegations of misuse of the internet.

Misuse Statement of Policy

St Francis' College will not tolerate illegal material and will report illegal activity to the Police and / or the Herts Safeguarding Children's Partnership. If the College discovers that a child or young person is at risk as a consequence of online activity it may seek assistance from the Child Exploitation and Online Protection Unit (CEOP). The College will use a range of sanctions on any pupil who uses technology to bully, harass or abuse another individual, in line with our anti-bullying and eSafety policies. This mistreatment includes activity outside of the school day.

Involvement of Parents and Guardians

The College seeks to work closely with parents and guardians in promoting a culture of eSafety. We will always contact you if we have any worries about your daughter's behaviour in this area, and we hope that you will feel able to share any worries with us. We recognise that not all parents and guardians may feel equipped to protect their daughter when they use electronic equipment at home. We therefore arrange discussion evenings for parents when specialist advice about the potential hazards of this exploding technology, and the practical steps that parents can take to minimise the potential dangers to their children without curbing their natural enthusiasm and curiosity. Mobile phone technology safety is also explored in ICT lessons as well as PSHE, tutor times and assemblies.

Charter for the Safe Use of the Internet and Mobile Devices.

"Children and young people need to be empowered to keep themselves safe. This isn't just about a top-down approach. Children will be children - pushing boundaries and taking risks. At a public swimming pool we have gates, put up signs, have lifeguards and shallow ends; but we also teach children how to swim."

(Dr Tanya Byron 'Safer Children in a digital world: the report of the Byron Review'.)

E-safety is a whole College responsibility, and at St Francis' College, the staff and pupils have adopted the following charter for the safe use of the internet inside the College:

Cyberbullying

- Cyberbullying is a particularly pernicious form of bullying, because it can be so pervasive and anonymous. There can be no safe haven for the victim, who can be targeted at any time or place. Our College's anti-bullying policy describes our preventative measures and the procedures that will be followed when we discover cases of bullying.
- Proper supervision of pupils plays an important part in creating a safe ICT environment at College; but everyone needs to learn how to stay safe outside the College.
- We value all of our pupils equally. It is part of the ethos of the College to promote considerate behaviour, and to value diversity.
- Bullying and harassment in any form should always be reported to a member of staff. It is never the victim's fault, and she should not be afraid to come forward.

Treating Other Users With Respect

- We expect pupils to treat staff and each other online with the same standards of consideration and good manners as they would in the course of face to face contact. They should always follow the College's Rules and Regulations set out in the Acceptable Use Policies a copy of which is in the homework diary.
- We expect a degree of formality in communications between staff and pupils, and would not allow them to communicate with each other by text or personal mobile phones. Our policy on Educational Visits explains the circumstances when communication by mobile phone may be appropriate. In such circumstances, [staff use College, as opposed to personal, mobiles and] pupils' mobile numbers are deleted at the end of the visit, and pupils are instructed to delete staff numbers.
- Everyone has a right to feel secure and to be treated with respect, particularly the vulnerable. Harassment and bullying will not be tolerated. Our Anti-bullying policy is set out in the Parent Handbook. The College is strongly committed to promoting equal opportunities for all, regardless of race, gender, gender orientation or physical disability.
- All pupils are encouraged to look after each other, and to report any concerns about the misuse of technology, or worrying issues to a member of staff.
- The use of cameras on mobile phones is not allowed in washing and changing areas or in the bedrooms of Boarding House.

The College recognises the role of mobile technology in the sharing of images, consensually and non-consensually and viewing adult material. Students are taught about safe online activity through the PSHE and ICT Curriculum, as well as in tutor time and assemblies.

The College recognises the potential for phones to be used for peer-on-peer abuse. The Peer-on-Peer Abuse policy should be read alongside this policy. The College will always act robustly when dealing with instances of peer-on-peer abuse on phones, even when undertaken outside of College.

Keeping the College Network Safe

- We adhere to best practice guidelines regarding e-teaching and the internet.
- Certain sites are blocked by our filtering system and our ICT Department monitors use of the network.
- The ICT Department monitors email traffic and blocks SPAM and certain attachments.
- We issue all pupils with their own personal College email address. Access is via personal LOGIN, which is password protected. We give guidance on the reasons for always logging off and for keeping all passwords securely.
- Access to sites such as "Hotmail" is not allowed on the College's network.
- We have strong anti-virus protection on our network, which is operated by the ICT Department.
- Staff and pupils are allowed to connect mobile devices to the College wireless network. To connect as a network client users must contact the ICT department who will check for anti-virus software.

Promoting Safe Use of Technology

The College takes part in the annual Safe Internet Day. Pupils of all ages are encouraged to make use of the excellent online resources that are available from sites such as:

- Childnet International (www.childnet-int.org)
- UK Council for Child Internet Safety (<http://www.education.gov.uk/ukccis>)
- Cyber Mentors (www.cybermentors.org.uk)
- Cyberbullying (www.cyberbullying.org)
- E-Victims (www.e-victims.org)
- Bullying UK (www.bullying.co.uk)
- CEOP'S Think U website (www.thinkuknow.co.uk)
- UK Safer Internet Centre ([https:// www.saferinternet.org.uk/about](https://www.saferinternet.org.uk/about))

During PSHE, ICT and cross curricular lessons pupils cover the different hazards on the internet, such as grooming, stalking, abuse, bullying, harassment and identity theft. Guidance covers topics such as saving yourself from future embarrassment, explaining that any blog or photograph posted onto the internet is there permanently. Anything that has been deleted may be cached in a search engine, company server or internet archive and cause embarrassment years later.

Safe Use of Personal Electronic Equipment

- Our guidance is that no one should put anything onto the web that they would not say to face to face.
- We offer guidance on the safe use of social networking sites and cyberbullying in PSHE and ICT lessons, which covers blocking and removing contacts from "friends lists".
- Our PSHE lessons include guidance on how pupils can identify the signs of a Cyber- stalker, and what they should do if they are worried about being harassed or stalked online.
- We offer guidance on keeping names, addresses, passwords, mobile phone numbers and other personal details safe. Privacy is essential in the e-world.

Considerate Use of Electronic Equipment

Mobile phones and other personal electronic devices provide potential to enhance teaching and learning and this provides additionally challenges for e-safety within the College.

- Use of mobile devices during lessons will be at the discretion of teaching staff.
- Staff may confiscate personal equipment that is being used inappropriately during the school day in accordance with guidance on confiscation in the behaviour policy.
- Sanctions may be imposed on pupils who use their electronic equipment without consideration for others.
- Pupils are responsible for the security of their own devices, the College cannot take responsibility for the loss of these devices.

Related Policies

- Anti-bullying Policy (including Cyberbullying)
- Behaviour Policy
- Checking Employees, Temporary Workers, Governors, Proprietors, Volunteers and Contractors
- Safeguarding and Child Protection Policy and Procedures (in addition to Keeping Children Safe in Education 2021)
- E-Safety policy
- Induction of New Staff, Governors and Volunteers in Child Protection

- Staff Code of Conduct, located within the Staff Handbook
- Taking, Storing and Using Images of Children
- Peer-on-Peer Abuse Policy

Authorised By	J Nichols
Effective From	September 2021
Next Review Due	September 2023