HOLY FAMILY CATHOLIC HIGH SCHOOL

ICT ACCEPTABLE USE POLICY
PUPILS & PARENTS

POLICY DATE: December 2016
REVIEW DATE: February 2021
REVIEW DATE: March 2025

ICT Acceptable Use Policy for pupils and parents

'Together we step out in faith, knowing that Christ is with us and united as a holy family.

We commit to ensure that each child realises their full potential, growing in wisdom and grace. Holy Family Catholic High School places Christ at the heart of everything we do and openly gives witness to the Catholic values of love, compassion, forgiveness, and reconciliation in our daily work.

Scope:

It is within this context that our ICT Acceptable Use Policy is written, the aim of which is to safeguard each member of the school community in order that they can realise their full potential – spiritually, academically, socially, morally and culturally, and 'increase in wisdom and grace'.

Holy Family Catholic High School takes the safety of all children and adults very seriously. This policy is written to protect all children and adults. We recognise that E-Safety encompasses not only Internet technologies, but also electronic communications such as mobile phones and wireless technology

"The Internet and related technologies are powerful tools, which open up new prospects for communication and collaboration. Education is embracing these new technologies as they bring with them fresh opportunities for both teachers and learners.

The online world develops and changes at great speed. New opportunities, challenges and risks are appearing all the time. This can make it difficult for schools to stay up to date with the latest devices, platforms, apps, trends and related threats. 20. It is therefore important to focus on the underpinning knowledge and behaviours that can help pupils to navigate the online world safely and confidently regardless of the device, platform or app". **DFE 2019**

The Holy Family Catholic High School promotes the use of technology in school, as all pupils will need the skills and knowledge in whatever field of work they enter when they become an adult. We ensure that our school IT network is robust and resilient and we do our upmost to ensure the safety of children when using it. It is important that pupils abide by the school rules when using technology in school and inform a member of staff immediately, if they become aware of any misuse.

This is the Acceptable User Policy (AUP) for our school. It highlights the do's/don'ts of using all technology in school and shows how we want pupils to behave when using IT. Any misuse will result in pupils being temporarily banned from using the school network. In addition, the AUP covers the following legislation:

- Malicious Communications Act
- 1988 Data Protection Act 1998
- Computer Misuse Act 1990
- Communications Act 2003
- Sexual Offences Act 2003

Using the school's IT systems and cloud-based subscriptions

Whenever you use the school's IT systems (including by connecting your own device to the network) or cloud-based subscriptions such as Office 365, you should follow these principles:

- Only access systems and software using your own username and password. Do not share your username or password with anyone else.
- Do not attempt to circumvent the content filters or other security measures installed
- on the school's IT systems, and do not attempt to access parts of the system that you do not have permission to access.
- Do not attempt to install software on, or otherwise alter, school IT systems.
- Do not use the school's IT systems in a way that breaches the principles of online behaviour set out above.
- Remember that the school monitors use of the school's IT systems, and that the school can view content accessed or sent via its systems.

Passwords

Passwords protect the School's network and computer system and are your responsibility. They should not be obvious (for example "password", 123456, a family name or birthdays), and nor should they be the same as your widely-used personal passwords. You should not let anyone else know your password, nor keep a list of passwords where they may be accessed and must change it immediately if it appears to be compromised. You should not attempt to gain unauthorised access to anyone else's computer or to confidential information to which you do not have access rights.

Use of Property

Any property belonging to the School should be treated with respect and care and used only in accordance with any training and policies provided. You must report any faults or breakages without delay.

Use of school systems

The provision of school email accounts, Wi-Fi and internet access is for official school business, administration and education. Staff and pupils should keep their personal, family and social lives separate from their school IT use and limit as far as possible any personal use of these accounts. Again, please be aware of the school's right to monitor and access web history and email use.

Monitoring and access

Staff, parents and pupils should be aware that school email and internet usage (including through school Wi-Fi) will be monitored for safeguarding, conduct and performance purposes, and both web history and school email accounts may be accessed by the school where necessary for a lawful purpose – including serious conduct or welfare concerns, extremism and the protection of others.

Any personal devices used by pupils, whether such use is permitted, may be confiscated and examined under such circumstances. The school may require staff to conduct searches of their personal accounts or devices if they were used for school business in contravention of this policy.

Compliance with related school policies

You will ensure that you comply with the school's e-Safety Policy, Safeguarding, Anti-Bullying and Acceptable Use Policy.

Breaches of this policy

A deliberate breach of this policy will be dealt with as a disciplinary matter using the school's usual procedures. In addition, a deliberate breach may result in the school restricting access

to school IT systems. If you become aware of a breach of this policy or the e-Safety Policy, or you are concerned that a member of the school community is being harassed or harmed online you should report it to a member of staff. Reports will be treated in confidence.

Please read carefully and sign at the bottom to show you agree to these terms. If you do not sign and return this form you will not be able to use the IT systems in school.

For Pupils:

Using Technology in Schools

- I will only use school Internet, IT facilities and mobile technologies for educational purposes, which follow the teachers' instructions. This includes email, video, messaging, video-conferencing, using software apps, social media, Internet, file-saving and printing.
- I will only use my mobile phone, mobile device or smart watch in school when a teacher has granted permission. If permission is granted, I will use my mobile device in line with how I would use other technology in school.
- I will not look at or delete or amend other people's work or files.
- I will treat all IT equipment at school with respect and ensure the computer or mobile device is left in the state that I found it.

Security, Passwords & Copyright

- I will not install software on school IT facilities due to the risk of damage being caused by malware or viruses. I will ask an ICT teacher or technician to install software if required.
- I will only install software apps on mobile devices when directed to by a teacher. I will only use school-related information when registering for an app.
- I will not share my network, Internet or any other school-related passwords.
- I will change my passwords when asked to and ensure that they have complexity e.g. Capital, lower case letters, numbers and symbols.
- I will only use my school-supplied email address for school-related activities.
- I will respect copyright when making use of images, videos or other media in my school work.
- I will use and attribute 'Creative Commons' material as taught in ICT/e-safety lessons.
- I will follow the school procedures when using removable media e.g. flash drives to ensure that I don't infect any machines.
- I will not look for ways to bypass the school filtering, monitoring or proxy service.
- I will not bypass the school filtering, monitoring or proxy service.

Online Behaviour & Safety

- I will make sure all my contact with other people at school is responsible. I will not cyber bully pupils, teachers or other members of staff.
- I will be responsible and polite when I talk online to pupils, teachers and other people related to the school, both in school-time and outside school-time.
- I won't look for or look at unpleasant, unsuitable or extremist websites in school. I will check with a teacher if I think a website might be unsuitable.
- I won't give out my personal details, such as my name, address, school or phone number on the Internet.
- I won't meet people I've met on the Internet unless I have told my parents and they come with me.
- I won't upload or download any pictures, writing or films which might upset people online.
- I won't write unpleasant, rude or untrue comments online about pupils, teachers or other staff employed by the school.
- I won't share inappropriate images or videos of other pupils on the school network or personal devices.
- I am aware that everything I do on the computers at school is monitored and logged, and that the school can talk to my parents if a teacher is concerned about my online safety or my behaviour when using school computers.
- I will not look for, view, upload or download offensive, illegal, copyright-infringing or

pornographic material. If I find such material on school IT equipment I will inform a teacher immediately.
- I understand that these rules are designed to keep me safe and that if they are not followed, sanctions may be applied and my parent/guardian may be contacted.

For parents:

As you are aware, mobile phone use within school is prohibited; therefore, it is the responsibility of the pupil to ensure that their mobile phone is out of sight and switched off throughout the school day. This policy is in place to ensure that; there are fewer distractions in the classroom, on the corridors between lessons and to act as a safeguarding measure with regards to unauthorised pictures being taken of pupils and inappropriate social media posts being made.

If there is an issue between pupils regarding social media, the school will endeavour to mediate between all parties involved. However, the school is not responsible for social media issues occurring 'out of school hours'. It is the responsibility of parents/carers to ensure that their child is using social media appropriately and to ensure that no harm, emotional or physical, is caused to others. Such offences would fall under the Communications Act (2003) and may require the intervention of the police.

Link to e-safety training for parents:

https://www.e-safetysupport.com/onlinetraining?course=tGgbQqEel85k&school=916

Further information can be found by visiting www.e-safetysupport.com

- I agree to support and uphold the principles of this policy in relation to my child and their use of the Internet& social media, at home and at school.
- I agree to uphold the principles of this policy in relation to my own use of the Internet & social media, when that use is related to the school, employees of the school and other students at the school.
- Images of pupils will only be taken, stored and used for school purposes in line with school policy. Images will only be used on the Internet or in the media with permission.

Signed: **Headteacher**