ICT & Acceptable Use Policy

Holy Family Secondary School

APRIL 2024

1. Link to School Mission Statement

This policy has been developed in line with our Mission Statement which states that:
'We promote the Christian virtues of faith, hope, love, gentleness, respect and tolerance, and we emphasise togetherness and family. Guided by these Christian virtues, and dedicated to the pursuit of excellence, it is our mission to provide a safe, caring, inclusive learning environment in which to foster the spiritual, intellectual, academic, aesthetic, physical, emotional, and social development of each pupil so that she may fulfil her own unique potential and may leave our school with the capacity and the willingness to contribute to the building of a society characterised by these Christian virtues.'

Acceptable use of school ICT is compatible with the Ethos of Holy Family Secondary School. An educational goal of this school is to promote and maintain a culture of digital citizenship and cyber-safety, that is in keeping with our school values and with legislative and professional obligations.

2. Rationale, Aims & Definitions

The aim of this ICT & Acceptable Use Policy is to ensure that students will benefit from learning opportunities offered by the school's Internet resources in a safe and effective manner. Internet use and access is considered a school resource and privilege. Therefore, if the school AUP is not adhered to this privilege will be withdrawn and appropriate sanctions – as outlined in this policy document – will be imposed. An acceptable Use Policy (AUP) is a document which addresses all rights, privileges, responsibilities, and sanctions associated with the internet. It is incorporated into the school's overall Information and Communications Technology (ICT) policy.

All users of our ICT infrastructure are responsible for seeing that our devices and systems are used in an effective and efficient manner for educational purposes, taking account of related ethical and lawful considerations. This document establishes the rules and restrictions, including what is prohibited, that define acceptable use of these devices and systems. Unacceptable use is prohibited and where deliberate misuse occurs, sanctions according to the school's Code of Behaviour and the relevant statutory laws apply. The purpose of Internet use in Holy Family Secondary School is to enhance learning through use of digital technologies, which is central to the National Digital Framework and embedded in subject specifications for the Junior Cycle. Furthermore, the internet is used to support the professional work of staff and to facilitate and enhance the overall management and administration of the school as an organisation.

Some Important Terms in this Document

- ***Cyber-safety*** refers to promoting safe use of the internet and protection against viruses, fraud, and other forms of threat.
- ***Cyber-bulling*** is bullying which uses electronic communication (i.e. public posts, chat, email, SMS text messaging, or similar mobile device applications used for instant messaging, social media applications or websites) to engage in bullying of a person, typically sending messages or creating digital content of an intimidating or threatening nature.
- ***ICT*** (Information and Communications Technology): Technologies that provide access to information through telecommunications.
- ***School's Digital Technologies Infrastructure (DTI)*** refers to the school's computer network, internet access facilities, telecommunications systems, computer software, the school's cloud storage and communications platform (Microsoft Office 365 for Education), computers and other ICT equipment or portable devices as outlined below.
- ***ICT equipment*** includes computer hard drive towers, monitors, keyboard, mice, portable devices, webcams, microphones, speakers, digital projectors, cameras or other devices used for the purpose of taking photos or video recording, digital recording devices, external storage devices such as flash drives or USBs, visualisers, printers, photocopiers, scanners, CD-players, telephone sets, mobile phones, WIFI access points, the school's computer server and any equipment used for and including wiring and cables for the ICT infrastructure in the school.
- ***Digital learning*** refers to the embedding of digital technologies within learning, teaching, and assessment practices in a school.
- ***Digital technologies*** can be defined as electronic tools, systems, devices, and resources that generate, store or process data including online games, online learning platforms and software applications.
- ***Inappropriate material*** means material that deals with matters of sex, cruelty or violence in a manner that is likely to be injurious to children or incompatible to a school environment.
- ***Electronic crime*** *(also known as cyber-crime or e-crime)* refers to any criminal activity, in which the internet and a computer or another electronic device are used either to commit and offence, are targeted in an offence, or are involved in any other way in such an offence.

3. Scope of this policy

This policy applies to all users of the ICT infrastructure of Holy Family Secondary School, both staff and students. This policy is to be read and interpreted in its totality and operates within the context of all Holy Family school policies and procedures. All school policies are available on our school website www.holyfamily.ie under the policy tab.

The policy also operates within a legislative framework and takes account of the following:

- The Education Act, 1998
- Data Protection Act, 1988
- Freedom of Information Act, 1997
- Video Recordings Act, 1989
- Interception of Postal Packets and Telecommunications Messages Act, 1993
- Child Trafficking & Pornography Bill, 1997
- The Education Welfare Act, 2000
- Equal Status Act, 2000
- The Equality Act, 2004
- Child Protection Guidelines for Post-Primary Schools, 2004

4. School vision for Digital Learning

The vision for digital learning in HFSS is for our students to be engaged in a purposeful academic environment and a challenging curriculum that is student-centred and focused on inquiry-based learning. We aim to harness the potential of digital technology to support new approaches to innovative learning centred on the development of 21st century learning skills. These include creativity and innovation; critical thinking, problem solving, decision making; life-long learning; collaboration and communication; digital literacy; consciousness of being a local and global citizen; and personal and social responsibility. We believe that every learner in HFSS is inspired and empowered to participate, contribute, and shape their own learning through digital technology.

The internet and use of digital technologies are essential elements of 21st century life for education, the world of work, social interaction, and European and global citizenship. The development of a national digital framework, *Digital Learning Framework for Post Primary Schools*, was a key objective of the *Digital Strategy for Schools 2015-2020 Enhancing Teaching, Learning and Assessment*. The Digital Learning Framework for post-primary schools provides a clear path and a set of standards for teachers to effectively embed digital technologies into their practice, and guides school leaders and school management in creating a shared vision for how digital technologies meet the requirements of learners in post primary education. In April, 2022 the Digital Strategy for Schools to 2027 was published and sets out objectives under three key pillars: **Pillar 1** Supporting the embedding of digital technologies in teaching, learning and assessment, **Pillar 2** Digital Technology Infrastructure and **Pillar 3** Looking to the future: policy, research and digital leadership. This document builds on the previous strategy to support schools to ensure that all learners have opportunities to acquire the knowledge and skills needed to navigate the ever-changing digital world, in which we live.

From this arises the need to plan for and integrate the use of digital technologies into classroom practice for the purpose of learning and safely navigating information on the internet, taking account of the risks and benefits of using the world wide web in the context of learning related to the school curriculum and in line with the national digital strategy.

The *Digital Learning Team* is a voluntary working committee comprised of the ICT coordinator, members of the school leadership team, and teachers with an interest in ICT and digital learning in the school. The aim of this team is to lead, manage and support the Digital Strategy for Schools to 2027 and the Digital Learning Framework which aims to embed digital technologies into the everyday life of the school, to support teaching and learning as well as leadership and management, and to plan for the effective practice of digital learning across the school. Holy Family Secondary School's *Digital Learning Plan* is updated yearly, and outlines the targets, actions, and outcomes for digital learning in the context of the academic year.

4.1 Outcome Statements (Digital Learning Plan)

- Access to and the use of digital technologies will become an integral part of education for our students.
- We endeavour to use communication and digital technologies to enhance and expand student academic fulfilment and to master 21st century skills, such as communication, collaboration, and critical thinking.
- Our students will learn and demonstrate competencies and understanding of aspects of digital technologies with the aim of becoming digitally literate, independent, confident, and discerning users of technology.
- Our students will acquire and develop critical and analytical attitudes to appropriately choose the right digital tools according to specific needs along their own learning journey.
- Our students will gain an understanding of the way in which digital technology operates in multiple contexts and how to utilise this learning to broaden their learning.
- Our school will embrace digital learning, so that classrooms and learning spaces become environments in which teachers and students are comfortable using digital technology and students take responsibility for their own learning.

4.2 Belief Statements (Digital Learning Plan)

- Consultation with stakeholders and the current context in our school will inform the direction of our Digital Learning Plan.
- Frequent opportunities for collaboration and reflection on the use of digital technologies are essential for teachers.
- Teachers must be supported to engage in a plan of continuous professional development in the use of digital technologies, in order to achieve curricular aims and further learning for students.
- Teachers should have access to technology and resources within the school, early in the planning process, in order to fulfil the targets and aims of the Digital Learning Plan in line with our national digital strategy.

4.3 Teacher professional development and training

- It is recognised that the work of teachers involves not only the use of digital technologies for learning, teaching, and assessment but also for whole school and departmental administrative tasks, curricular planning, collaboration, and communication.
- The work of the Digital Learning Team includes setting targets and outcomes related to continuing professional development for teachers in the use of digital technologies. These outcomes and targets form part of the Digital Learning Plan.
- Through the integration of the School Self Evaluation process (SSE), individual and whole staff needs are identified. Surveys on the use of digital technologies and feedback on previous CPD experiences are used to determine shortfalls in teacher professional development.
- Progress is monitored through a staff mentoring system and feedback. Further surveys are used to identify subsequent CPD requirements for staff.
- Ongoing professional development for teachers on the use of digital technologies, blended, remote, and digital learning is supported by Oide (formerly the PDST Technology in Education) and can be accessed at www.teachercpd.ie and local education centres, for example, www.eckildare.ie.
- Professional development on the use of digital technologies, which may be delivered internally by HFSS teachers or externally by outside agencies, is regularly supported and facilitated by the senior leadership team and other school leaders of HFSS. The frequency and amount of such professional development will depend on the needs of the school or any changing national educational context at the given time.

5. Use of and Access to Digital Technologies & ICT Resources

- There are two computer rooms with 30 desktop computers in each.
- First years are timetabled in the computer rooms for *Digital Media Literacy and Guidance* for one hour per week.
- All TY students are timetabled in the computer room for *Digital Portfolio & Skills* for one hour weekly.
- Career guidance and LCVP classes are timetabled in the computer rooms for one hour weekly.
- Other subjects, such as LCPE, 6th year Research Skills, Graphics and some TY modules, are also timetabled in the computer rooms at regular intervals.
- All students have an opportunity to access the computer rooms over the academic year with their subject teachers – access to computer rooms operates either on a rotated timetable or on a weekly booking system.
- Each classroom has a desktop computer, digital overhead projector or interactive TV display, and internet access. These resources are used for learning activities every day in the classroom and are mainly teacher-led.
- All classroom computers have a webcam, with microphone built in to it, which can be used for Junior Cycle assessment and Leaving Cert assessment where audio-visual recording is required. There is at least one tablet device for each subject department in Junior Cycle, for use by teachers and, where required, students (under teacher supervision), for the purpose of Junior Cycle Assessment (CBAs, SLARs) and any teaching and learning activities leading up to these assessment periods.
- There are three class sets of tablet devices, stored in charging trolleys, which may be used for teaching, learning and assessment in the classroom. Access to these devices operates on a rotated timetable or on a weekly advance booking system.

- All students and teachers have both an account on our school platform, Microsoft Office 365, and an individual login to the school network.
- All subject class groups have a class team in Microsoft Teams for communication and learning. Some teachers use One Note Class Notebook, and/or other Microsoft Apps, in addition to Teams.

5.1 ICT Curriculum

- All first-year students are timetabled for *Digital Media Literacy & Guidance*, in line with the Wellbeing guidelines. *D(M)LG* aims to develop personal, social, and cultural literacy and skills related to the areas of both Digital Media Literacy and Guidance.
- All TY students are timetabled for *Digital Portfolio & Skills* in Transition Year, where they have an opportunity to build an online portfolio of their work, keep a digital blog of their learning and TY experience, carry out project work for subject teachers, explore digital tools, engage in reflection, learn about digital literacy and critical thinking skills and other digital skills relevant to the online space.
- Some TY students are learning the basics of coding in TY Maths classes with Java programming.
- Senior Cycle programmes such as Senior Cycle Physical Education and LCVP have an ICT course component.

5.2 Health & Safety Considerations for Use of ICT

- Both computer rooms have suitable workstations with sufficient space between students for comfortable working position. Students are encouraged to sit up straight when working on computers in the school building.
- In the case of the need for a significant period of remote learning, guidelines for timetabling include an extended lunch break, reduced class periods of 50 minutes (from 60 minutes) to allow for movement breaks, time away from the screen and a short break between online lessons. Students are encouraged to take breaks away from the screen when working online at home.
- If learning online from home, students should ensure, where possible, that they have a suitable workspace at a table or desk, and to ensure good posture when working on their device.
- Mobile phones are not recommended for long periods of online learning from home. If possible, a desktop computer, laptop computer or tablet device should be used instead.
- Computer room protocols are clearly visible in both computer rooms and on the mobile class set of HP devices.
- No eating or drinking is permitted beside school ICT equipment, as this is an electrical hazard.
- Trailing cables in classrooms are secured and covered, and school bags are stowed neatly under desks to avoid trip hazards.
- Paper and other flammable materials are kept away from school ICT equipment, as this is a potential fire hazard.
- Computer rooms are ventilated regularly to avoid overheating of computers.
- All classroom computers, school devices, printers, photocopiers, interactive TV displays and projectors are switched off at the end of the school day.

For further information on health and safety in HFSS, please refer to the school Health & Safety Policy available on our school website at www.holyfamily.ie/policy

5.3 Digital Technologies for School Communication & Administration

- Our Office 365 platform is used for all school communications. Outlook is used for email communication. Teams is used for communication, dissemination of information, file storage and collaboration.
- Working groups in HFSS, such as committees and teams use Outlook Groups and/or Teams for effective communication, collaboration and sharing of files.
- Subject Departments communicate through both Outlook and Teams. Teams is used by subject departments for file sharing, collaboration, subject planning, and department meetings.
- Whole school documents and information is stored and disseminated by email (Outlook) and/or by Teams on Office 365. Administration staff also use the school network for file storage and sharing.
- The school Information Management System used in HFSS is VS-ware. This system is used for recording student attendance, the storage of timetables and class lists, student assessment results, and school reports.

- The Holy Family Secondary School mobile phone application (School App) is administrated by Unique schools and other designated members of staff. The School App is used for permission to leave from parents and for personal notification to parents from members of school management, as well as for posting news and general information to the school community.
- The school website and social media accounts are administered by Holy Family Secondary School. Publications on our school website and social media are moderated by members of the Senior Leadership Team and designated members of the Middle Leadership Team, such as the school PRO.

5.4 Digital files for Submission to State Examinations Commission

- In conducting video and/or audio recordings for the SEC, the procedures to be followed should be in accordance with the instructions and/or guidance for recording, issued by the Department of Education & Skills and/or the State Examinations Commission, and/or in line with Holy Family Secondary School's Acceptable Use Policy.
- In the case of recording audio-visual or audio material for submission to the State Examinations Commission, all video and audio recordings will be made on networked school devices. Specific computer logins for the school network will be created for the purpose of such examinations. All recordings must be removed as soon as possible from the school device and stored, according to the instructions and/or guidance for recording, issued by the Department of Education & Skills and/or the State Examinations Commission, and/or in line with Holy Family Secondary School's Acceptable Use Policy.
- For the purposes of GDPR compliancy, and in conjunction with the school Acceptable Use policy, no personal devices are to be used for the recording or storing of such material.

5.5 Junior Cycle CBAs: Storage of student samples of work from Classroom Based Assessments

- Teachers should only use school devices for audio/video recording of Classroom Based Assessments. Using personal devices for such purposes is not permitted. The storage of school-related data and samples of student work on personal devices, which are outside of both the school network and the school's designated cloud-based storage and communications platform (Microsoft Office 365) breaches GDPR roles and responsibilities for teachers https://gdpr4schools.ie/pdf/TeachingStaff.pdf
- For the purposes of audio/video recording, teachers may use either the desktop computer in the classrooms, using the webcam for audio/visual recording, a mobile school device or subject department tablet.
- Any files pertaining to CBAs should be uploaded to our cloud-based school platform, Microsoft Office 365, and stored in Teams within the subject department team, or in a separate department team created for the purpose of Junior Cycle assessment.
- These files should be stored until such time as the SLAR has been completed. Once the SLAR has been completed, any student data relating to the CBA should be deleted and removed from our school network or cloud-based platform.
- Each subject department may retain some samples of student work from the CBA, for the purpose of building up a bank of samples of work to be used for teacher professional development within the department and for subsequent SLAR meetings. These samples should be stored within the subject department team (Microsoft Office 365/Teams) in a secured folder, accessible only to teachers within that subject department.
- For GDPR reasons, if a teacher or student needs to log in to their Office 365 school account using the subject department device or classroom computer, and where it is not possible to use their individual network login, they should open a new *private or incognito window* in the web browser, rather than signing into Office 365 Apps such as Outlook, One Drive, Teams etc.

5.6 Security of School Network & School Platform

- On the school's network, content on the internet is filtered through the PDST Content Filtering Service (now Oide), which is currently set at level 4. Level 4 filtering allows access to most content on the web, including You Tube, but blocks access to websites belonging to the 'personal websites' category and 'social networking' category. *'Content filtering is an essential and integrated element of the broadband service that is provided to schools by the Schools Broadband Programme. The purpose of Content filtering is to ensure (in so far as possible) that inappropriate websites and content are not accessible from within schools.'*

  https://www.pdsttechnologyineducation.ie/en/Technology/Schools-Broadband/Content-Filtering/

- ***Microsoft Office 365 Education*** is a collection of online services that allows students to collaborate and share their schoolwork. It includes Outlook, Word, Excel, PowerPoint, OneNote, Publisher, and Access. In addition, Office 365 Education includes classroom tools such as Exchange, OneDrive, SharePoint, Skype for Business, Teams, Sway, Forms, Stream, Flow, PowerApps, School Data Sync, and Bookings.

  https://privacy.commonsense.org/privacy-report/Microsoft-Office-365-Education

- The security and compliance features that come as standard with the free Office 365 Education subscription include features such as threat management, mobile device management, data loss prevention, data governance, search and investigation, Office 365 secure score, service assurance, and compliance manager. *Threat management* can help protect inbound and outbound messages from malicious software, and can also be used to protect from spam, protect the domain's reputation and to determine whether or not senders are maliciously spoofing accounts from your domain. *Data loss prevention* can identify, monitor, and automatically protect sensitive information across Office 365. It works across SharePoint, OneDrive and Exchange Online.

- The school's DTI, internet and network facilities, and the student school accounts on our school's cloud-based storage and communications platform (Microsoft Office 365 for Education) are owned and operated by Holy Family Secondary School and as such the school reserves all rights, including termination of service without notice, to the ICT infrastructure that it owns and operates. These procedures shall not be construed as a waiver of any rights of the school, nor shall they conflict with applicable acts of law. Rigorous practices are in place in Holy Family Secondary School, which include the school's Anti-bullying Policy for staff and pupils, who have been involved in the development of the agreement.

6. User Agreement

The user agreement should be read carefully to ensure that the conditions of use are understood and accepted.

All students and members of staff have access to the school network, the internet, school devices, and our school cloud storage system and communications platform, Microsoft Office 365, which includes free downloads of Office 365 software applications to personal devices at home.

All users of Holy Family Secondary School's Digital Technologies Infrastructure must read, understand, and comply with the policies outlined in this document, as well as any additional guidelines established by school management, in consultation with staff and pupils.

Staff Acceptable Use of ICT

6.1 Staff Acceptable Use of ICT

Staff should note the below best practice and procedures:

- ✓ Teachers are aware that access to digital resources and the use of digital tools on the internet are intended to enrich learning activities and encourage students to engage in the appropriate use of such resources and tools, in line with our school Acceptable Use Policy, for their subject learning.
- ✓ Teachers guide students to use online activities that are appropriate to their age and stage of learning and students are supported by their teachers to achieve planned learning outcomes related to the specification or syllabus, through effective use of digital technologies.
- ✓ Teachers expect students to conduct themselves responsibly when using technology through devices and the internet. Teachers guide and encourage students to become good digital citizens, with the support of the school's code of behaviour, antibullying policy and this AU Policy.
- ✓ Students are made aware that they must immediately report any damage to the school's ICT equipment to their teacher. All issues with the school's Digital Technology Infrastructure should be recorded by teachers in Teams, as per our agreed standard procedures.
- ✓ All users of the school's Digital Technologies Infrastructure will observe good netiquette and online ethics in line with the school's Acceptable Use Policy.
- ✓ **All teachers must have an individual computer login for the school network.** Users should keep school passwords and login details secure. All users are responsible for keeping their own login details for their school account on Microsoft Office 365. Any issues with school accounts or passwords should be reported directly to the ICT coordinator.
- ✓ All users have access to the school network via their individual computer logins (username and password). Any issues related to login details, needed to access school devices on our school network, should be reported directly to the ICT coordinator.
- ✓ Users are aware that all school communications on Office 365 remain the property of the school and that, should the need arise, any communication on our school platform - for example in Teams (posts or chat) or in Outlook (emails) - may be accessed and inspected at any time, and without prior notice to the user.
- ✓ All files should be stored on the user's One Drive, the cloud storage system on the school's Microsoft Office 365 platform. Using a cloud storage system invalidates the use of external/removable storage devices, which may contain viruses and can be harmful to the school's DTI.
- ✓ Teachers should routinely ensure that all school-related documents are uploaded to their Office 365 account (One Drive cloud storage) to ensure that their documents are both secure and retrievable.
- ✓ Teachers should log off computers at the end of class, for GDPR reasons, and shut down the computer and projector at the end of the day. The projector should be switched off when not in use.
- ✓ Staff should respect the rights of all online and in our school community and recognise that any inappropriate online behaviour or cyber-bullying will not be tolerated and will result in sanctions, and that this includes bullying or behaviour that is homophobic, related to race or ethnicity, or directed at any minority group in our school community.
- ✓ Messages and emails to other users and parents/guardians are always professional in tone and content, and the language of such communications are respectful and appropriate for school communication.
- ✓ Teachers always acknowledge the use of other people's ideas, knowledge, and sources and all materials and sources are appropriately referenced.

6.2 Staff Unacceptable Use of ICT

It is not permitted for staff to do the following:

- Retrieve, print, copy, display, share or forward offensive messages or images in any school communication.
- Use obscene, homophobic, or racist language in any school communication.
- Harass, insult, attack, intimidate others in any communication or engage in any form of cyber bullying.
- Break or misuse the school's Digital Technologies Infrastructure in any way that may result in damage or poor functionality.
- Violate copyright laws by copying, saving, downloading, printing, or redistributing copyright-protected material.
- Engage in plagiarism. Plagiarism is when someone passes off someone else's work as their own.
- Access and encroach on another user's files or emails, without their permission.
- Use the school's Digital Technologies infrastructure for unapproved commercial or personal purposes, or personal profit, financial gain, gambling, political purposes, or advertising.
- Visit websites or internet applications with obscene, illegal, hateful, or otherwise inappropriate material. If a member of staff receives any offensive or intimidating material via school communication, or in a pop-up window, it should be reported immediately, providing details to the ICT coordinator.
- Get involved in any activities that may be considered an e-crime (criminal activity that involves the internet and a computer or other device).
- Subscribe to or order any services or products, on the school's behalf, without prior approval from the principal.
- Publish, save, download, share, forward or re-distribute any personal information about another user, such as personal contact information or images.
- Read, copy, manipulate or edit messages or emails intended for another user, or impersonate another user on Office 365.
- Open or click on links in any suspicious emails from users outside the organisation. You should instead delete any such emails immediately and report any issues of this kind to the ICT coordinator.
- Deliberately visit, view, or download any material, from any website or web application, containing illegal material of an offensive, discriminatory, or sexual nature.
- Download any software or applications on school devices, without permission.
- Engage in or support cyber-bullying activities or behaviours.
- Use removable storage devices, such as USBs or external hard drives on any school ICT equipment, as viruses can attached themselves easily to such devices.
- Consume food or drinks directly beside any school ICT equipment, for health and safety reasons.
- Make use of school printers/photocopiers for inappropriate or personal use.
- Use another network login, other than the one that has been assigned, to access the school network.
- Share their login details with another user or use another user's login details to access the school's Digital Technologies Infrastructure.

Student Acceptable Use of ICT

Each year, parents/guardians of incoming first year students are made aware of and asked to support the school's ICT & Acceptable Use Policy. Students will be presented with an 'Acceptable use of ICT agreement' in the school journal. Parents/guardians and incoming first-year students are required to read and sign the agreement. Subsequently, the user will have access to the school's Digital Technologies Infrastructure. Parents/guardians are informed in the case that their child is found to be in breach of the Acceptable Use of ICT Agreement. **In using the school's Digital Technologies Infrastructure, it is to be clearly understood that an agreement is automatically entered into that all users will agree to comply with both the acceptable use guidelines in the school journal and this policy.**

6.3 Student Acceptable Use of ICT

Students should note the below best practice and procedures:

- ✓ Students' access to digital resources and the use of digital tools on the internet are intended to enrich learning activities, and students will be familiar with appropriate use of such resources and tools, in line with our school Acceptable Use Policy.
- ✓ Students will be guided by teachers to engage with online activities that are appropriate to their age and stage of learning and will be supported to achieve planned learning outcomes related to the specification or syllabus, through effective use of digital technologies.
- ✓ Students are expected to conduct themselves responsibly when using technology through devices and the internet. Teachers will guide and encourage students to become good digital citizens, with the support of the school's code of behaviour, antibullying policy and the AUP.
- ✓ Students must immediately report any damage to the school's ICT equipment to their teacher.
- ✓ Users of our school's ICT infrastructure will observe good netiquette and online ethics in line with the school's Acceptable Use Policy.
- ✓ Students should keep school passwords and login details secure. Students are responsible for keeping their own login details for their school account on Microsoft Office 365. Any issues with school accounts or passwords should be reported to the teacher, class tutor, year head or directly to the ICT coordinator.
- ✓ All students have access to the school network via their individual computer logins (username and password), or the generic student login details displayed in computer rooms. Any issues related to login details, needed to access school devices on our school network, should be reported directly to the ICT coordinator.
- ✓ Students should be aware that all school communications in Office 365 remains the property of the school and that, should the need arise, any student communication on our school platform - for example in Teams (posts or chat) or in Outlook (emails) - may be accessed and inspected at any time, and without prior notice to the user.
- ✓ All files should be stored on the user's One Drive, the cloud storage system on the school's Microsoft Office 365 platform. Using a cloud storage system invalidates the use of external/removable storage devices, which may contain viruses and can be harmful to the school's DTI.
- ✓ Students should routinely ensure that all school-related documents are uploaded to their Office 365 account (One Drive cloud storage) to ensure that their documents are both secure and retrievable.
- ✓ Students must ask permission from a teacher to print material in the computer rooms.
- ✓ Students should log off devices at the end of the class and shut down devices at the end of the day.
- ✓ Students should respect the rights of all online and in our school community and recognise that any inappropriate online behaviour or cyber-bullying will not be tolerated and will result in sanctions, and that this includes bullying or behaviour that is homophobic, related to race or ethnicity, or directed at any minority group in our school community.
- ✓ Students should be careful when wording messages and emails to other users: students must always ensure that the tone, content, and language of such messages are respectful and appropriate for school communication.
- ✓ Students must always acknowledge the use of other people's ideas, knowledge, and sources, to avoid plagiarism. All material and sources should be clearly referenced when submitting any essays, tasks, assignments, or projects to the teacher.

6.4 Unacceptable Use of ICT

It is not permitted for students to do the following:

- Use mobile phones in school: the school currently operates an off and away policy on use of mobile phones.
- Use a personal laptop, mobile or tablet devices in school, without permission from the ICT coordinator, SEN coordinator, or a member of the Senior Leadership Team.
- Use the school's Digital Technologies Infrastructure without permission or supervision from a member of staff.
- Retrieve, print, copy, display, share or forward offensive messages or images in any school communication.
- Use obscene, homophobic, or racist language in any school communication.
- Harass, insult, attack, intimidate others in any communication or engage in any form of cyber bullying.
- Break or misuse the school's Digital Technologies Infrastructure in any way that may result in damage or poor functionality.
- Attempt to fix any school ICT equipment or plug in/out any cables on school ICT equipment.
- Violate copyright laws by copying, saving, downloading, printing, or redistributing copyright-protected material.
- Engage in plagiarism. With increased use of the internet for tasks and project work, and the ease at which information can be copied and pasted from the internet, plagiarism is becoming increasingly problematic in secondary schools. Plagiarism is when someone passes off someone else's work as their own. This practice is not tolerated in Holy Family Secondary School.
- Access and encroach on another user's files or emails, without their permission.
- Use the school's Digital Technologies Infrastructure for unapproved commercial or personal purposes, or personal profit, financial gain, gambling, political purposes, or advertising.
- Visit websites or internet applications with obscene, illegal, hateful, or otherwise inappropriate material. If a student receives any offensive or intimidating material via school communication, or in a pop-up window, it should be reported immediately, providing details to the teacher, the class tutor, or the year head.
- Get involved in any activities that may be considered an e-crime (criminal activity that involves the internet and a computer or other device).
- Engage with any activities that may bring the Holy Family Secondary School into disrepute, including using the school's name, or part thereof, to create any digital content, for example, videos, podcasts, websites, web pages, blogs, vlogs, or online social media accounts. The school retains the right to its own online identity and parents/guardians are requested to support the school in this matter.
- Use the school's Digital Technologies Infrastructure for purposes unrelated to education, by searching for, viewing, downloading, or printing material not related to schoolwork or the aims of the curriculum and without approval or instruction from the teacher. This may include, for example, playing games online, watching videos, listening to music, accessing social media websites, online shopping etc.
- Subscribe to or order any services or products, on the school's behalf, without prior approval from the principal.
- Publish, save, download, share, forward or re-distribute any personal information about another user, such as personal contact information or images.
- Search for the personal details or online profiles of any staff member of Holy Family Secondary School. All staff members are entitled to their online privacy.
- Friend or follow any member of staff via that staff member's personal online profiles. This applies to any personal accounts on social media, music, video or professional networking platforms, web sites or web applications.
- Read, copy, manipulate or edit messages or emails intended for another user, or impersonate another user on Office 365.
- Open any suspicious emails from users outside the organisation. You should instead delete any such emails immediately and report any issues of this kind to the ICT coordinator.

- Deliberately visit, view, or download any material, from any website or web application, containing illegal material of an offensive, discriminatory, or sexual nature.
- Download any software or applications on school devices, without permission.
- Engage in or support cyber-bullying activities or behaviours.
- Use removable storage devices, such as USBs or external hard drives on any school ICT equipment, as viruses can attached themselves easily to such devices.
- Consume food or drinks in either of the computer rooms or directly beside any school ICT equipment, for health and safety reasons. Standard operating procedures for student use of room 36 and 41 are clearly displayed in both computer rooms.
- Make use of school printers/photocopiers for inappropriate or personal use.
- Share their login details with another user or use another user's login details to access the school's Digital Technologies Infrastructure.

6.5 Violations & Sanctions

- School accounts on Office 365 www.office.com are owned and administrated by Holy Family Secondary School and Wriggle Learning Ltd. Students should be aware that all activity on student accounts is monitored, files may be inspected or removed, and any inappropriate use or any serious breach of the school's AUP will result in sanctions, which may include the student account being suspended or the removal of the student from the Office 365 platform.
- All staff at Holy Family Secondary School are entitled to their privacy and good name and should not be harassed, bullied, commented upon, or abused online or on any social media website or internet application. This will be considered a serious breach of the HFSS Code of Behaviour and the HFSS Anti-Bullying Code. The rights of all are respected in Holy Family Secondary School.
- Any misuse of the school's identity will be a matter for consideration with the Board of Management and any persistent or abusive violation of the school's name will be taken very seriously and will result in serious sanctions for those students involved.

7. Advice for Parents/Guardians

7.1 Responsibilities of Parents/Guardians

Parents have a responsibility to support student learning at home, which may regularly include the use of digital technologies. Digital technologies are part of learning in the 21st century and are embedded in subject specifications and learning outcomes for both Junior and Senior Cycle programmes.

Teachers will use a blended learning approach to design in-class learning activities and homework. As such, students must have access to the internet and a suitable device to fully engage with homework, learning activities, projects, and tasks that are routinely assigned in all school subjects. Students should be encouraged and supported by parents/guardians to regularly check the school platform Office 365, Teams and/or Class Notebook (One Note) to keep up with learning activities in class and homework.

In the case of school closure, or a remote learning situation due to health and safety, students are expected to attend online classes and access classwork and homework via our school platform Office 365 www.office.com and our designated school learning hub, *Teams*. Parents/guardians are responsible for supporting students to access learning from home via our school Office 365 platform, which includes ensuring access to the internet and a suitable working device.

Parents/guardians are responsible for the safekeeping of all passwords related to the following:

- ✓ payment of school fees
- ✓ access of information, such as school reports and exam results, on the school's management information system, *VS-ware*
- ✓ logging on to the school learning platform, Office 365 www.office.com (particularly for parents/guardians of first year students). Student passwords can be reset by contacting a teacher, the class tutor, year head or the ICT coordinator directly.

7.2 Acceptable Use & Internet Safety

Please take the time to read this ICT & Acceptable Use Policy with your child and support the school in maintaining appropriate and respectful practices and behaviours online. You may refer to www.dataprotection.ie for further information about acceptable use.

It is acknowledged by HFSS that students use the internet at home and outside of the school setting for communication, online gaming, and social media networking. It is important that parents also talk to their child about the potential dangers of online activities including cyberbullying and internet safety while accessing the internet outside of school hours. Parents/guardians will find some helpful resources to deal with cyber safety at the below weblinks:

https://www.webwise.ie/internet-safety-talks-for-parents/

https://www.pdst.ie/sites/default/files/Parents%20guide%20to%20safer%20internet.pdf

8. Websites for Additional Resources & Supports

- The Professional Development Service for Teachers (PDST) www.pdst.ie and www.oide.ie
- Web wise is the Irish Internet Safety Awareness Centre, co-funded by the Department of Education & Skills and co-financed by the EU's Connecting Europe facility. It is part of the PDST Technology in Education, a part of the PDST (now Oide), which promotes and supports the integration of Digital Technology in teaching and learning in secondary schools www.webwise.ie and www.pdsttechnologyineducation.ie
- Office of internet safety (Department of Justice) www.internetsafety.ie
- Data Protection Commissioner www.dataprotection.ie

9. Review and Ratification

This policy was reviewed and ratified by the Board of Management of Holy Family Secondary School at its meeting on 23rd April 2024

Signature: _____ Date: _____

Chairperson, Board of Management

Signature: _____ Date: _____

Diocesan Representative

Signature: _____ Date: _____

Principal