**Holy Spirit Girls’ National School**

 **Acceptable Usage Policy (AUP)**

**Rationale**

The aim of this Acceptable Usage Policy (AUP) is to ensure that students will benefit from learning opportunities offered by the school’s ICT and internet resources in a safe and effective manner.

In addition, this AUP aims to support the Department of Education and Skills’ (DES) vision for the integration of ICT into Irish schools,

 “To realise the potential of digital technologies to enhance teaching, learning and assessment, so that Ireland’s young people become engaged thinkers, active learners, knowledge constructors and global citizens to participate fully in society and the economy”

*(DES, p. 5, 2015).*

Internet use and internet access is a school resource and privilege.

Therefore, if the school AUP is not adhered to, this privilege will be withdrawn and appropriate sanctions will be imposed.

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

**School Strategy**

The school employs a number of strategies, taking into account the age of the pupils, in order to
maximise the learning opportunities and to reduce the risks associated with accessing the internet, namely, exposure to inappropriate online content and cyberbullying.

The strategies include:

* Internet access will always be supervised by a teacher. The content will be subject to the restrictions of the automated web-filtering function from the Professional Development Services for Teachers (PDST) Technology in Education. The purpose of content filtering is to ensure (in so far as possible) that both inappropriate websites and content are not accessible from within schools. - See more at: <http://www.pdsttechnologyineducation.ie>.
* Holy Spirit Girls’ National School holds a Level 3 web-filtering function for pupils which blocks YouTube and Social Networking sites from use, and a Level 4 web-filtering function for teachers which enables them access to YouTube for educational purposes.
* If a teacher wishes to integrate YouTube into a lesson, it must be fully previewed and evaluated for inappropriate advertising content, imagery, and text, prior to usage.
* Pupils will treat others with respect at all times and will not undertake any actions that may bring the school into disrepute.
* Virus protection software will be used and updated on a regular basis.
* Holy Spirit Girls’ National School uses ‘G Suite for Education’ to enable pupils from Junior Infants- 6th Class to access education productivity tools from Google, including Docs, Classroom, and Slides. Pupils will use their G Suite accounts to complete assignments, communicate with their teachers and peers, and learn 21st century digital citizenship skills.

**Pupils’ Use of the Internet**

1. *World Wide Web*
* Pupils who have access to the internet will do so in adherence to the above strategies.
* Websites that the children use in school/ at home will be previewed by their teacher before use, and subject to the filters operated by the PDST and Schools Broadband programme.
* Teachers and pupils will be familiar with copyright issues relating to online learning, for example, ensuring images used in projects are not copyrighted. Teachers and pupils are encouraged to use https://search.creativecommons.org/ to search for images.
* Pupils will never disclose or publicise personal information.

  *2. Internet Chat / Social Networking / Instant Messaging (IM)*

* Access to internet chat rooms, social networking sites, and instant messaging services is
forbidden and blocked in accordance with the Schools Broadband Internet Policy.

 *3. Email*

* Pupil’s have no access to email services through Google to ensure Child Safeguarding guidance is followed.

4*. School Website*

* Pupils will be given the opportunity to publish projects, artwork, or school work on [www.holyspiritgns.ie](http://www.holyspiritgns.ie) in accordance with this policy and approval processes, regarding the content that can be loaded to the school’s website.
* The website will be moderated to ensure that there is no content that compromises the safety of pupils or staff.
* The publication of pupil work will be co-ordinated by a teacher and authorised by the school.
* Pupils’ work will appear in an educational context. Pupils will continue to own the copyright of any work published.
* The school will endeavour to focus on group activities when using digital photographs, audio or video clips. Content, focusing on individual pupils, will not be published on the school website without parental consent.
* Personal pupil information including home address and contact details will be omitted from school web pages.

*5. iPads/ Tablets/ Laptops/ Desktops*

* Currently there are 8 iPads for use within the classroom setting.
* All the above devices are on level 3 automated filtering service from the PDST as previously stated.
* All iPads have parental controls activated and apps have been selected for educational purposes only. Apps are installed by the IT administrator only, and pupils are unable to access the app store on these devices themselves.
* Unless previously authorised by a teacher, pupils’ personal devices are not to be used on school premises. If a pupil needs to bring a device to school, a Parent/ Guardian should provide a note explaining why the device is required and both note and device handed to the classroom teacher.
* The unauthorised capture of images, video or audio is in direct breach of the school’s AUP.
* Connecting to or attempting to connect to the school’s network system without authorisation, is in direct breach of the school’s AUP.

 *6. Plagiarism*

* Pupils should not plagiarise content (copy or use your own without citing the original creator), including words or images from the internet for inclusion in school blogs/ projects.
* Pupils should not take credit for things they didn’t create themselves, or misrepresent themselves as an author or creator of something found online.
* The school will encourage pupils who create original content to claim ownership of it.

 *7. Cyberbullying*

 Understanding Cyber Bullying:

* Cyber Bullying is the use of ICT (usually a mobile phone and/or the internet) to abuse or harm another person.
* It can take place anywhere, and can involve many people.
* Any person can be targeted, including pupils, school staff, and members of the wider school community.
* It can include threats, intimidation, harassment, cyber-stalking, vilification, defamation,
exclusion, peer rejection, impersonation, and unauthorised publication of private
information or images.

There are many types of cyber-bullying. The more common types are:

1. Text messages – can be threatening or cause discomfort. Also included here is
‘Bluejacking’ (the sending of anonymous text messages over short distances using
Bluetooth wireless technology)
2. Picture/video-clips via mobile phone cameras – images sent to others to make the victim
feel threatened or embarrassed.
3. Mobile phone calls – silent calls, abusive messages or stealing the victim’s phone and using it to harass others, to make them believe the victim is responsible.
4. Emails – threatening or emails of a bullying nature, often sent using a pseudonym or somebody else’s name.
5. Chat room bullying – menacing or upsetting responses to children or young people while
they are in a web-based chat room.
6. Instant messaging (IM) – unpleasant messages sent while children conduct real-time
conversations online using MSM (Microsoft Messenger), Yahoo Chat or similar tools.
7. Bullying via websites – use of defamatory blogs (web logs), personal websites, gaming
websites, and online personal ‘own web space’ sites such as YouTube, Facebook, Instagram, Twitter, and SnapChat, among others.

Procedures for preventing Cyber Bullying:

1. Staff, pupils, parents, and Board of Management (BOM) are made aware of issues
surrounding cyber bullying.
2. Pupils and parents will be urged to report all incidents of cyber bullying to the school.
3. Pupils will learn about cyber bullying through Social, Personal and Health Education
(SPHE), and other curriculum projects.
4. All reports of cyber-bullying will be noted and investigated, in accordance with the school’s Anti-Bullying, and Child Protection Policies, where applicable.

**Distance Learning**

This section sets out the policy of the school in respect of use of technology for distance or remote teaching and learning during potential Coronavirus stay at home instruction, hereafter referred to as “Distance eLearning”.

In all cases students must use their @holyspiritgns.ie account to log in. Students are not to use any other account under any circumstances for the purposes of Distance eLearning within the school.

The list of applications that will be used for distance learning will primarily be:

1. *Google Classroom*
2. *Zoom*

**eLearning Approach**

eLearning will take what is known as a blended approach and some teachers may use different methods more than another teacher. For example:

* Some teachers may use regular live classes while others may not
* Some teachers may use recorded videos of lessons
* Some teachers may distribute work as weekly bulk assignments while others may do so as daily homework-style tasks.

In all cases the primary aim is to cover the required curriculum areas for their specific subject. The teacher will decide the most effective method to use to achieve this aim. Students should get in touch with their teacher right away if they are having difficulty with any aspect of their subject or if they are finding the workload unmanageable.

**Everyone’s Responsibilities while partaking in eLearning**

For staff and teachers:

1. Teachers have overall control of the online interaction of their class
2. Disruptive students will be removed in order to allow those who wish to partake a fair chance to do so. Repeatedly disruptive students may receive a temporary ban from all online access.

For students:

1. You are to communicate through your @holyspiritgns.ie account only. The use of any other account or e-mail address is expressly prohibited
2. Do not engage in communications with any account other than an @holyspiritgns.ie account and report any such activity to your teacher
3. You must always be civil and respectful to your teachers and fellow students

For parents:

1. You should ensure that you or your child is checking in regularly for assigned work
2. Where live classes are being run you should ensure your child is in an area of the house that is quiet and free from distractions. Please be mindful of Child Protection Guidelines
3. Live online classes should be viewed by your child only.

**Live Online Classes**

Teachers may deliver some of the course “live” using Zoom. This will use varying combinations of audio, video, virtual whiteboards and screencasts.

In the use of Zoom:

1. Students must always follow the direction of their teacher just as in the classroom
2. Students are not to turn on their microphone unless the teacher invites them to do so. In any case, all microphones should be on mute when a person is not speaking to avoid distracting background noise being broadcast to everyone.
3. A Zoom is intended for the student only. The teacher will decide who should receive the link. Do not forward any link to anyone else.

**Data Privacy Statement**

What we retain:

* Login activity, specifically, the last time a student logged in to their Google Classroom account
* Within Google Classroom , the date and time of if/when a student views any assignments

Why we retain it:

* To assist us in making sure students are engaging in learning sufficiently and in good time
* To assist us in generating appropriate and relevant feedback to parents on progress
* To provide a record of activity in the event of a disciplinary or other issue arising during a live class.

Where we retain it:

* All recordings are kept within the School’s own systems which requires a valid @holyspiritgns.ie login to access

How long we retain it for:

Activity and content will not be retained beyond the students exit from the School, either through early exit or through graduation.

**Legislation**
- Data Protection (Amendment) Act 2003
- Child Trafficking and Pornography Act 1998
- Interception Act 1993
- Video recordings Act 1989
- The Data protection Act 1988

**Sanctions**

Misuse of ICT and internet resources may result in disciplinary sanctions, including written warnings, withdrawal of access privileges and, in extreme cases, suspension or expulsion.

The school also reserves the right to report any illegal activities to the appropriate authorities.

**Ratification by Board of Management**

This AUP was ratified by the Board of Management on \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ and will be reviewed in \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, or earlier if deemed necessary.

Carmel Terry:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(Chairperson)

Emma Conroy:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(Principal)

Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_