ACCEPTABLE USE OF I.T. (EMAIL, INTERNET & WEBSITES)
ST. GABRIEL'S SCHOOL POLICY

Aim

The aim of this policy is to ensure that pupils will benefit from learning opportunities offered by the school digital resources in a safe and effective manner. Internet use and access is considered a school resource and privilege. If the school Acceptable Use Policy is not adhered to this privilege may be withdrawn and appropriate sanctions will be imposed.

Whole - School Strategies

The school will employ a number of strategies in order to maximise learning opportunities and reduce risks associated with the Internet. These Strategies are as follows:

- The school will use the filtering software and/or equivalent system provided by the National Centre for Technology Education (NCTE) in order to minimise the risk of exposure to inappropriate material.
- Internet sessions are supervised by an adult.
- Students and teachers are made aware of guidelines relating to internet safety.
- Uploading and downloading of inappropriate software is not permitted.
- Virus protection software will be used and updated on a regular basis.
- All USB devices should be scanned before use.
- School cameras are provided for each class.
- The only phone allowed for photographs of children or events is the school mobile phone.
- School laptops normally remain on school premises. Exceptions may happen in line with the SEN policy.
- School tablets, iPads and other portable devices are solely for use in school and may only be taken home by staff members with permission from the Principal.
- Internet safety lessons are taught routinely as part of the school SPHE programme.
- Should Child Protection issues arise, the school will follow the Child Protection Policy and Children First National Guideline.

Responsibilities of Employees

Employees will:

- Follow the guidelines set forth in this policy.
- Supervise student use of the internet.
- Model and provide instruction in the ethical and appropriate use of technology in school
- Maintain a curricular focus
- Keep the user names and passwords secure and confidential
- Ensure the computers are being legally used according to the software's licence
- Only install software onto a school computer or network, which has been approved by the staff member with responsibility for ICT or the Principal
- Transmit, request or receive materials that are consistent with the mission and values of our school.
- Use the school email address assigned to them for school related business. Staff members should be aware that this address is the property of the school and can be accessed as necessary by the school authorities.
- Refrain from using mobile phones during class or supervision time. This includes texting, social medial, photography, information searches, etc.

- Be aware that personal phones and mobile devices are the employees own responsibility and should be stored safely and securely during the school day.
- Refrain from posting photographs of staff social events on the internet or social media.

Acceptable Use of Information Technology

Computers and networks are to be used in a responsible, efficient, ethical and legal manner and must be in support of the educational objectives of our school. Management reserves the right to monitor this usage. Incidental personal use of school devices may be permitted with express permission from the Principal as long as it use does not interfere with the employee's job, duties and performance with system operations or other system users. 'Incidental personal use' is defined as use by an individual employee for occasional personal communications. Employees are reminded that such personal use must comply with school policy and must take place outside of class times.

Unacceptable Use

This includes but is not limited to the following:

- Accessing, transmitting, or receiving obscene or pornographic material
- Engaging in cyber cheating or plagiarism. Plagiarism is material created by others and presenting it as if it were one's own
- Accessing the Internet for non-school related activities, such as chat rooms, engaging in instant messaging, shopping, posting or filling out forms with private or personal information about yourself or another person.
- Using mobile phones during class or supervision time.
- Downloading or uploading software or applications on to school devices without permission from the Principal/IT coordinator.
- Covert photographing or recording of others, using any device.
- Using school email addresses for non-school business

The above provide general guidelines and examples of prohibited uses for illustrative purposes, but do not attempt to state all required or prohibited activities by users. Staff and students who have questions regarding whether a particular activity or use is acceptable should seek further guidance from the Principal.

Student strategies

Use of the Internet

- All student use of the internet should be supervised.
- The internet should be used for educational purposes only.
- Students should not visit internet sites or search for sites that contain obscene, illegal, hateful or otherwise objectionable materials.
- Students may not record staff or other students unless permission is given by a teacher and the activity is supervised.
- Students should be familiar with copyright issues relating to online learning.
- Students should keep all personal information private.
- Students should be aware that any usage, including distributing or receiving information, school-related or personal, may be monitored for unusual activity, security and/or network management reasons.

- The schools Code of Behaviour may be applied for all inappropriate use of IT
- See below for a copy of the rules for children. These are explained annually.

Use of Email

- Students will use approved class email accounts under supervision from a teacher only.
- Sending and receiving email attachments is subject to permission from the teacher.
- Students will not send, receive or post any material illegal, obscene, defamatory or that which is intended to annoy or intimidate another person.
- Students must keep their own or other people’s personal details, such as addresses or telephone numbers or pictures private.
- Students must never arrange a face- to-face meeting with someone by using school email.
- Students will note that sending and receiving email attachments is subject to permission from their teacher.
- Students will not forward email messages or screenshots of emails or “reply all” without the permission of the originator.
- Students must only use their school email for school related activities and for registering on school based activities only. The use of personal email addresses is not allowed for school based work.
- Students should not use school email accounts to register for online services, social networking, apps or games.
- Students should report the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Students should report any such communications to a teacher Students should avoid opening emails that appear suspicious.
- Students should report any suspicious emails to a teacher.
- All emails and opinions expressed in email are the responsibility of the author and do not reflect the opinion of the school.

School Website

- Pupils may be given the opportunity to publish projects, artwork or school work on the school Website or blog pages, subject to resource availability and at the discretion of the school.
- The publication of student work will be co-ordinated and supervised by a teacher. Permission must be given by a teacher for all content uploaded to a blog page.
- Personal pupil information including home addresses and contact details will be omitted from the school Web pages.
- Pupil names must not accompany photographs on the school website or Blog pages.
- Care should be taken when taking photographic or video images that students are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.

- Students and staff must not take, use, share, publish or distribute images of others without their permission.
- Taking photos or videos on school grounds or when participating in school activities is only allowed with expressed permission from staff.
- Students and staff must not take or share images, videos or other content online with the intention to harm another member of the school community regardless of whether this happens in school or outside.
- Sharing explicit images and in particular explicit images of students and/or minors is an unacceptable, illegal and absolutely prohibited behaviour, with serious consequences and sanctions for those involved. Sharing explicit images of other students automatically incurs suspension as a sanction and will be reported to the appropriate authorities

Mobile Phones And Other IT devices

- Children's personal devices are not used for teaching & learning
- Children's personal mobile phones must be powered off and kept in school bags on entering the school grounds
- Mobile phones may not be used by children during the school day, except in an emergency and with the permission of a teacher.
- If a teacher has a suspicion that a mobile phone has unsuitable material stored on it, pupils will be required to hand over the phone to a teacher and parents will be asked to collect it.
- See the school Code of Behaviour for further information

Social Media

- The use of chat rooms and social media in school is prohibited.
- Inappropriate postings regarding school staff will be subject to the school Code of Behaviour sanctions.
- Children may not post photographs of school staff on the internet for any reason.
- On-line bullying by children will be dealt with under the school's Code of Behaviour.

Children's Rules for Using the Internet

1. The internet may only be used for educational purposes.
2. All internet use must be supervised by an adult.
3. You must have permission from your teacher to send an e-mail, make a posting or upload a photograph.
4. Open an e mail/attachment only when you are supervised by an adult.
5. Keep personal details about yourself (addresses, telephone numbers or pictures) private.
6. Chat rooms and social media e.g. Facebook, Snapchat, Instagram, may not be used in school.
7. The teacher or Principal may check the work you have done or the website you have visited.
8. Report messages or anything else that make you feel uncomfortable.

Photography

- Only school cameras may be used for taking photographs of children. If consent is given by the Principal, teachers may use their own cameras in exceptional circumstances. The use of staff mobile phones for photography is strictly prohibited.
- Children may not take photographs on their own phone, iPod, tablet, etc. at any time.
- Permission must be given by parents before photographs of children are placed on the school website, local newspaper – this is done on enrolment and can be withdrawn at any time.
- Permission for the use of photographs for publication in any circumstances other than those listed above must be sought separately each time.
- Parents are requested not to upload school photographs or video footage of other people's children in school events to social media networks.
- It is the policy of the school to use some photographs of children for some school displays
- Only teachers and SNA's will use cameras on school trips. Only school cameras may be used.
- Children may photograph each other only with permission from teachers and for specific purposes. Only school cameras may be used.

Video calls with children.

Please be aware that St. Gabriel's school cannot accept responsibility for the security of online platforms, in the event that they are compromised. Parental permission is implied, as the link to the call will be communicated via the parent/guardian's email address or Aladdin account. Essentially, by virtue of the pupil logging on to the call, permission is assumed and you are agreeing to the following policy, procedures and rules:

Parents and Guardians

1. It is the responsibility of parents and guardians to ensure that pupils are supervised while they are online.
2. The main purpose of a video call is to maintain a social connection between school staff and pupils and to encourage participation in online learning.
3. Be aware that when participating in group video calls, you can be seen and heard unless you are muted or have disabled your camera.
4. Please ensure that your child is on time for a scheduled video.
5. Make sure to familiarise your child with the software in advance. For video in particular, show them how to mute/unmute and turn the camera on/off.
6. Participants in the call should be dressed appropriately.
7. An appropriate background/room should be chosen for the video call.
8. Calls may not be recorded by participants although they may be recorded by the school for child protection/health and safety purposes only.
9. For detailed information on GDPR and Zoom, please visit https://zoom.us/privacyrule
10. Parents are asked to discuss and explain the rules listed below with their children.

Children

1. Pictures or recordings of the video call are not allowed.
2. Remember our school rules - they are still in place, even online.
3. Set up your device in a quiet space, with no distractions in the background.
4. Join the video with your microphone muted.
5. Raise your hand before speaking, just like you would do in class and use kind friendly words.

6. Show respect by listening to others while they are speaking.
7. Ensure that you are dressed appropriately; don’t meet your class on line in your pyjamas!
8. Be on time - set a reminder if it helps.

It is important to note that any breach of the above guidelines may result in a discontinuation of this method of communication. A breach may also result in a person being immediately removed from a meeting or a meeting being immediately terminated. The school’s AUP, Child Protection and GDPR policies apply.

Legislation

The school will provide information on the following legislation relating to use of the internet which teachers, students and parents should familiarise themselves with:

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

Other Relevant Policies

- Code of Behaviour and Anti-bullying
- Educational Trips
- Health & Safety
- Admissions and Participation
- Social Personal & Health Education
- Data Protection
- Child Protection

Use of IT devices at home

This policy applies equally to devices provided by the school/DES for home learning or on-line teaching and learning.

Sanctions

Misuse of the internet or IT devices by staff or students may result in disciplinary action (see Circular 60/2009). The school also reserves the right to report any illegal activities to the appropriate authorities.

REVIEW

This policy will be regularly reviewed by the Board of Management in accordance with experience and the requirements of any legislation. It shall be revised in full in at least 4 years.

SIGNATURE

Signed on behalf of the Board of Management

Patricia Slorin

Chairperson of Board of Management

Date: April 8th 2025

Appendix 1

Guidelines for school staff initiating and using Zoom

- Staff members are required to set up a Zoom account using their school address and become familiar with all the features.
- When meeting children on Zoom 2 adults are preferred at all times, one to lead and one to monitor.
- Recording is permitted for H&S only. There is a record button you can press if you feel the situation merits it e.g. for child protection issues
- Schedule short sessions – max 30 minutes
- When scheduling a meeting, set the following parameters: mute all participants on entry, allow participants from Ireland only, allow participants to join any time, host video on, host audio mute on entry. Enable waiting room.
- For behaviour management purposes, do not allow children to use the chat box.
- Activities should be prepared in advance .
- Aim to hold at least one Zoom call per class per week.
- Schedule a meeting and send invitations via Aladdin to relevant parents and the second adult.
- Staff may come to school to hold Zoom meetings if a suitable space/broadband is not available at home
- **Note**: Our GDPR, AUP and Child protection policies and usual professional standards and apply.