

Acceptable Use Policy

Presentation Girls' School values the use of the internet as an opportunity for learning. The aim of this policy is to promote the use of the internet as a valuable learning resource in a safe and effective manner. This Acceptable Use Policy has been produced by our teachers, Board of Management and parents and will be updated and reviewed regularly.

This Acceptable Use Policy is built on the following core principles:

- Internet use is planned, task-orientated and of educational benefit within a regulated and managed environment and is always supervised by the teacher.
- Methods to identify, assess and minimise risks will be reviewed regularly.
- Department of Education and Skills filter from the NCTE and anti-virus are in place
- Blocking strategies maintained by the Administrator prevents access to a list of unsuitable web sites.
- Pupils will be taught what to do if they experience material that they find inappropriate.
- Staff will take appropriate measures if they encounter material they deem to be inappropriate for use in school.
- Pupils will treat others with respect at all times and will not undertake any actions that may bring the school into disrepute.
- Work will be uploaded daily on See Saw/Aladdin Connect for pupils who are well and isolating due to Covid 19. This work should be reviewed by parents.

Remote Teaching and Learning Protocols for Pupils

- In the event of remote Teaching and Learning being deemed necessary by the school: See Saw and Aladdin Connect are the platforms that will be used by teachers to upload work and assignments and communicate with parents / guardians. The school reserves the right to change learning platforms if the school deems it necessary at a future date.
- School policies:
 - Code of Behaviour
 - Anti- Bullying Policy
 - Acceptable Use Policyapply to all school communication during periods of Remote Teaching and Learning.
- Pupils are expected to present assignments to the best of their ability where circumstances allow during periods of Remote Teaching and Learning.

Presentation Girls' School, Maynooth

How this will work for parents / guardians:

- Parents / Guardians will be asked to provide consent for use of See Saw app by their daughter.
- Pupils will be issued with an individual code at set up. This code is a unique identifier and should never be shared.
- Work will be set by teachers using the See Saw learning platform.
- Teachers will provide a bank of home learning activities, ideas and resources to include use of pupil texts and/ or on-line resources. The work will include pre-recorded instructional videos on activities to complete.
- Teachers will request work to be submitted for review using either video – recording, audio recording, photographs or direct input on See Saw platform.
- Teachers will identify the specific piece of work to be submitted for review each day.
- If pupil has a difficulty in accessing activities on See Saw, please contact the teacher or the school.
- We understand that engagement with learning activities may not always be possible.

How this will work for pupils:

- Each pupil will be issued with set pieces of work on See Saw to complete on a daily basis. One piece of specified work can be sent to the teacher for review.

How this will work for teachers:

- All teachers will provide work for pupils to complete at home.
- Teachers will identify the specific piece of work to be submitted for review each day.
- Teachers will review and respond to pupils' work.
- Teachers will endeavour to differentiate learning activities to the pupil's abilities.
- Presentation Girls' School GDPR policy will be strictly adhered to in protecting personal data of pupils and parents/ guardians.
- The normal school calendar applies during periods of Remote Teaching and Learning.

Zoom:

In the event of Zoom contact deemed necessary by the school: Zoom will be used to ensure regular contact with pupils and to maintain a sense of connection to the class, the teacher and the school. Protocols for Parents / Guardians, pupils and teachers regarding the use of Zoom have been established. All parties must agree to the protocols set out below.

Presentation Girls' School, Maynooth

Protocols for Parents / Guardians for Pupil Zoom calls

Please note Zoom calls are not for instructional purposes.

1. Parental /Guardian agreement with Zoom call protocols and parental / guardian consent for pupil participation in Zoom calls is required.
2. Under no circumstances can photos, screenshots or recordings be taken of Zoom video calls.
3. Zoom calls are subject to the school's Acceptable User Policy (available on school website), Anti-bullying Policy and Code of Behaviour. In such instances where it is deemed that breaches of school policy have occurred pupils may be excluded from future Zoom meetings and parents may be contacted and informed.
4. Pupils are expected to behave in an appropriate, safe, respectful and courteous manner online during the Zoom call.
5. Zoom calls should take place in a quiet environment, free from other distractions such as mobile phones or electronic devices and with a neutral backdrop. (Identifying images should not be visible).
6. A Zoom link is intended for the pupil only to access the Zoom call and must not be forwarded or shared with anyone else.
7. Pupils will automatically enter a waiting room when the code for a Zoom call has been entered. Please note that school staff will only accept users into Zoom video call if the pupil can be identified by the display name submitted by parent in advance with consent to participate. (A Zoom account should not be set up for children under the age of 16 in compliance with Zoom terms and conditions).
8. Please request to join the Zoom call approximately five minutes before the scheduled start time.
9. Please make your daughter (s) aware that when participating in group Zoom video calls, they can be seen, and also heard by all participants when unmuted by the teacher.
10. Cameras must be turned on for all pupil participants and the pupil visible on screen at all times. If not visible on the screen pupils will be excluded from the Zoom call.
11. It is required that parent/guardian is present in the room to supervise their daughter while a Zoom call with the class teacher.

Presentation Girls' School, Maynooth

12. Presentation Girls' School cannot accept responsibility for the security of online platforms, in the event that they are hacked.
13. The criteria for mandated Child Protection reporting remains the same as if the child was being taught in school.
14. It is at the teacher's professional discretion to terminate a Zoom call should the need arise or dismiss participant (s) from the meeting.
15. All provisions relating to the child's data remains the same under GDPR procedures and guidelines
16. For detailed information on GDPR and Zoom, please visit <https://zoom.us/privacy>

Protocols for Pupils Participating in Zoom calls

1. Pupils are expected to behave in an appropriate, safe, respectful and courteous manner online during the Zoom call. This live class meeting requires the same high standards of behaviour as are expected in school.
2. Zoom calls are subject to the school's Acceptable User Policy (available on school website), Anti-bullying Policy and Code of Behaviour. In such instances where it is deemed that breaches of school policy have occurred pupils may be excluded from future Zoom meetings and parents may be contacted and informed.
3. Under no circumstances can photos, screenshots or recordings be taken of Zoom video calls.
4. A Zoom link is intended for the pupil only to access the Zoom call and must not be forwarded or shared with anyone else.
5. Please request to join the Zoom call approximately five minutes before the scheduled start time.
6. Cameras must be turned on for all pupil participants and the pupil visible on screen at all times. If not visible on the screen pupils will be excluded from the Zoom call.
7. Please remember that when participating in group Zoom video calls, pupils can be seen, and also heard by all participants when unmuted by the teacher.
8. Pupils should be aware that voices will be muted on admission to meeting until individually unmuted by the teacher and invited to contribute if they so wish.

Presentation Girls' School, Maynooth

Protocols for Teachers using Zoom calls to class:

1. Teachers will communicate with pupils and families during the hours of 9.00am – 2.40pm.
2. Teachers will check that consent and agreement to Protocols have been provided, along with the user name / parent email account from which pupil will log in, before issuing an invitation to a Zoom meeting.
3. Any class division will be based on alphabetical order of pupil surnames.
4. Teachers will provide a Zoom link via Aladdin Connect/See Saw with details of date, time and password for each Zoom video call.
5. All pupils will automatically be muted and teachers will unmute / mute individual pupils as necessary.
6. Teachers will have high expectations regarding pupil behaviour while participating in online communication.
7. It is at the teacher's professional discretion to terminate a Zoom call should the need arise or dismiss participant (s) from the meeting.
8. Teachers will report any concerns regarding online behaviour or interactions to school management.
9. Teachers will only admit participants to video conferences if they recognise the username as being connected to a pupil.
10. The criteria for mandated Child Protection reporting remains the same as if the child was being taught in school.
11. Under no circumstances can photos or recordings be taken of video calls.

Usage of school's computers, network and internet facilities by pupils:

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

- Internet sessions will always be supervised by a teacher.

Presentation Girls' School, Maynooth

- Internet access will be planned to enrich and extend learning activities. Access levels will be reviewed to reflect the curricular requirements and age of pupils.
- Staff will guide pupils in on-line activities specific to the learning outcomes planned for the pupils' age and maturity and curricular area.
- Pupils will be encouraged to be critically aware of the materials they read before accepting its accuracy.
- Pupils will be taught to acknowledge the source of information and to respect copyright when using Internet material in their own work.
- Filtering software will be used in order to minimize the risk of exposure to inappropriate material.
- The school will regularly monitor pupils' Internet usage.
- Students and teachers will be provided with training in the area of Internet safety.
- Uploading and downloading of non-approved software will not be permitted.
- Students may use approved class email accounts under the supervision of the teacher.
- The use of DVDs or USB storage devices in school requires a teacher's permission.
- Pupils are not permitted to access 'Chat Rooms' or social networking sites in the classroom/in the school.
- Pupils are not permitted to intentionally visit Internet sites containing objectionable materials.
- Although the school actively seeks to promote the safe use of the Internet, it recognises the possibility that pupils may accidentally access objectionable material. Should such an event occur pupils will be taught to:
 - Minimise the screen immediately. Turn off the monitor
 - Report to the teacher
 - Teacher logs/notes name of the site
 - Report to Principal/Administrator and site will be blocked
- Parents /legal guardians will be immediately informed.
- Pupils will never disclose or publicise personal information.
- Pupils will 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.

Consequences of inappropriate usage by pupils

Where a breach of inappropriate use is suspected or is alleged to have occurred, a thorough and transparent investigation of the matter will take place. All details will be recorded. This investigation will be carried out by the Administrator or Principal and appropriate action will be taken. Misuse of the internet may result in

Presentation Girls' School, Maynooth

disciplinary action including a written warning, withdrawal of access privileges, detention or in serious instances may result in expulsion or dismissal in accordance with the school's Code of Behaviour.

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

Usage of school's computers, network and internet facilities by staff:

- Staff utilise the school's computers, networks and Internet services for school-related and educational purposes.
- Teachers are provided with IT devices for teaching and learning of pupils and requisite school planning. The use of these devices is restricted to the above purpose. All such devices are signed in and returned to the I.T. Co-ordinator at the end of the school year, or completion of contract.
- Staff is made aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Staff is expected to use appropriate judgment and caution in communications concerning pupils and staff to ensure that personally identifiable information remains confidential.
- Copyright, intellectual property rights and the correct usage of published materials will be respected.
- Email is used to communicate to others on work-related matters

Consequences of inappropriate usage by staff

Should the user's conduct in relation to the use of email, internet or web browsing be deemed inappropriate (by the Administrator, the I.T. Co-ordinator, the Principal or Board of Management) a thorough investigation will take place.

Failure to comply with this policy may result in disciplinary action up to and including expulsion or dismissal in accordance with the DES Circular 60/2009.

Roles & Responsibilities:

Pupils and staff will act responsibly at all times when on the Internet and will not undertake any unauthorized actions that may bring the school into disrepute.

The Principal is responsible for

- ensuring that all staff, students and parents are aware of the existence of this policy
- ensuring that all teachers are aware of the content of this policy and of their responsibilities under this policy as users of the system
- initiating a review of this policy in due course.
- engaging a professional educator in internet safety to provide a workshop for the pupils in 5th and 6th class. A parent talk may also be provided by the same facilitator on request.

Presentation Girls' School, Maynooth

The Board of Management seek the support of parents in the proper education of children in the use of electronic devices. The Board of Management further requests the co-operation of parents in promoting the responsible use of such devices in school and at home.

The Administrator and I.T. Co-ordinator is responsible for

- encouraging staff members to plan and implement the e-learning programme as laid down by the NCTE in their e-learning roadmap for schools.
- ensuring that all teachers using the computer facilities to teach others are aware of the content of the policy and aware of their responsibility to secure the signatures of parents on the Internet Permission form.
- monitoring overall use of computers by staff while respecting the privacy of individuals. The initial investigation of any alleged breach of the policy, passing on relevant information to the Chairperson of the Board of Management, Deputy Principal or Principal as appropriate and co-operating with any further investigation being carried out by the appropriate authorities.

Individual Teachers are responsible for

- ensuring that good practice in the use of the internet is taught to pupils
- ensuring that their pupils are made aware of the content of the policy
- securing the signatures of parents on the *Internet Use Policy*
- filing the agreements securely as directed by the Principal and
- passing on details of any alleged breach to the Administrator and I.T. Co-ordinators in a timely fashion

Parents are responsible for ensuring that

- they discuss the contents of the policy with their child
- they sign the policy together with their child
- their child returns the signed policy to the school in good time

Pupils are responsible for ensuring that

- they are familiar with and abide by the content of the policy
- they report any breach of their own or that of others they discover in the course of using a computer.

Legislation

There is no specific legislation governing internet safety at school level. The following pieces of legislation have relevance to internet safety:

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

Presentation Girls' School, Maynooth

Complaints regarding Internet use:

Complaints of a child protection nature must be dealt with in accordance with The Department of Education and Skills 'Child Protection Procedures for Primary and Post Primary Schools'.

Responsibility for handling incidents will be delegated to Designated Liaison Person (The Principal) and / or the Board of Management.

Pupils and parents will be informed of the complaints procedure.

SOCIAL MEDIA GUIDELINES

These guidelines and A.U.P. have been developed to assist all employees of Presentation Girls' School (hereinafter referred to as "the School") in making ethical, respectful and acceptable decisions about their professional and personal social media usage and to provide clear direction on the importance of protecting the School's reputation and confidential information.

Social media refers to social and professional networking platforms such as Facebook, Twitter, WhatsApp, YouTube, LinkedIn, Snapchat, Instagram, blogs, message boards and forums and other similar online facilities.

The guidelines and A.U.P. are not intended to prevent employees from engaging in social media but are intended to inform employees as to what is considered by the School to constitute appropriate / inappropriate social media usage and conduct.

For those employees who are members of the School's teaching staff, the guidelines and A.U.P. give effect to agreed professional protocols as prescribed by the Code of Professional Conduct for Teachers (Teaching Council, June 2012) which provides that teachers should: -

"ensure that any communication with pupils/students, colleagues, parents, school management and others is appropriate, including communication via electronic media, such as email, texting and social networking sites."

and

"ensure that they do not knowingly access, download or otherwise have in their possession while engaged in school activities, inappropriate materials/images in electronic or other format."

All employees should be mindful of what they post on social media, who can see it and how it can be linked back to the School and work colleagues. Misuse of social media can cause injury to others and can have a negative impact on the reputation of the School. Social media communications are never truly private and once information is published it becomes part of a permanent record.

Presentation Girls' School, Maynooth

Employees are **at all times prohibited from using or publishing information on social media which has the potential to negatively impact / reflect on the School and / or its employees and / or its students e.g.:** -

- publishing defamatory, abusive or offensive material concerning any employee, volunteer, member of School management, parent(s), student(s), visitor or other member of the School community;
- publishing any confidential or sensitive information concerning the School or members of the School community;
- publishing material that might reasonably be considered to have the effect of damaging the reputation of the School.

The School reserves the right to take disciplinary action, up to and including dismissal, in respect of employees who engage in prohibited conduct and conduct in breach of this policy.

Given the ever developing and changing nature of social media and the internet the within guidelines and policy will be reviewed and adapted as required.

This policy should be read in conjunction with staff policies which are applicable to social media usage, in particular the dignity at work, data protection, the Code of Professional Conduct for Teachers and other and disciplinary policies and procedures.

ACCEPTABLE USAGE POLICY

A. SOCIAL MEDIA USAGE ON A SOCIAL MEDIA SITE OR PROFILE ESTABLISHED IN THE COURSE OF EMPLOYMENT WHICH RELATES TO SCHOOL BUSINESS / MATTERS

- Seek permission:** Employees must seek or have permission from the Principal / Deputy Principal(s) before setting up a site or profile relating to School business and or School matters / registering in the School's name on social media sites, user groups, special interest forums and bulletin boards / using social media for teaching and learning purposes.
- Property:** The property rights in a sanctioned social media account in the name of or on behalf of the School are vested in the School.
- Responsibility:** A permitted employee is responsible for his/her social media usage, for ensuring that private and confidential information is respected and protected at all times and for compliance with the terms and conditions of the relevant social media platform.
- Privacy & Confidential information:** Confidential information pertaining to the School, its employees, volunteers, students, parents and others in the School community must be respected and maintained at all times. Personal information about any students, parents, employees or volunteers must not be divulged or discussed on social media sites.

Presentation Girls' School, Maynooth

- v. **Unacceptable use:** Employees must not create, publish, download or communicate material/content that could reasonably be regarded as defamatory, inappropriate, discriminatory, offensive, hostile, pornographic, damaging to the School's reputation or referring to a third person without their permission. Uploading, forwarding or linking to the aforementioned content is also unacceptable. Employees must never reveal sensitive details whether relating to the School, its employees, volunteers, students, parents and other members of the School community on social media sites.
- vi. **Behaviour:** Postings by an employee on a social media site that are defamatory, inappropriate, discriminatory, offensive, hostile, pornographic, divulging personal data without consent or damaging to the School's reputation will be addressed pursuant to the School's disciplinary procedure and may result in disciplinary sanction up to and including dismissal.

B. PERSONAL SOCIAL MEDIA USAGE

- i. **Boundaries:** Personal profiles are not to be used to conduct school business or to communicate with students/parents. Online interaction with management, other employees and/or school contacts should be appropriate and professional in nature. Employees must not use the official School e-mail address when participating in personal social media / social media that is not related to the employee's job. Personal use of social media must not occur during working time but is restricted to break times at work.
- ii. **Identity:** Where an employee chooses to identify him/herself on social media as an employee of the School, s/he must make it clear that their communications do not represent the School, its ethos, position, opinions or views. The employee must write in the first person and state clearly s/he is posting in a personal capacity and not in the course of employment or on behalf of the School and state clearly that the views expressed are his/her own and not those of the School. Employees should at all times be mindful of their communications and possible consequences.
- iii. **Be mindful and respectful:** Employees must be mindful that their conduct not only reflects on themselves but also reflects on their professionalism and the School. Employees should exercise sound judgement, common sense and respect when participating in social media. Employees should not use insulting, offensive or disparaging language. If in doubt, don't publish or post anything. Information published online is permanent and never completely private.
- iv. **Responsibility:** Employees are personally responsible for their posts and actions on social media.
- v. **Privacy & Confidential information:** The obligations detailed at (A)(iv) above apply also to employees' personal social media usage. Do not divulge or discuss confidential information pertaining to the School, its employees, volunteers, students, parents and others in the School community and personal information, including photographs, of third persons (including employees, students, parents and other members of the School community)

Presentation Girls' School, Maynooth

- must not be posted, divulged or discussed without the permission of the person concerned.
- vi. **Unacceptable use:** Employees must not create, publish, download or communicate material/content that could reasonably be regarded as defamatory, inappropriate, discriminatory, offensive, hostile, pornographic, damaging to the School's reputation or referring to a third person without their permission. Uploading, forwarding or linking to the aforementioned content is also unacceptable. Employees must never reveal sensitive details whether relating to the School, its employees, volunteers, students, parents and other members of the School community on social media sites.
 - vii. **Behaviour:** Postings by an employee on a social media site that are defamatory, inappropriate, discriminatory, offensive, hostile, pornographic, divulging personal data without consent or bring the School into disrepute will be addressed pursuant to the School's disciplinary procedure and may result in disciplinary sanction up to and including dismissal.

REPORTING

Employees should immediately report to the Principal / Deputy Principal any inappropriate, abusive or defamatory or other unacceptable social media activity concerning the School, its employees, volunteers, students or other members of the School community. Such reports will be fully and confidentially investigated, the reported activity will be reviewed and, where appropriate, the content will be reported using the relevant online reporting mechanism.

ENFORCEMENT

The School will monitor social media usage on School computers, laptops, mobiles, tablets, notebook computers, smartphones, School accounts and School user names. The foregoing IT resources are the School's property and are to be used for legitimate School business. Whilst the School will not specifically monitor social media for references to the School, its employees, volunteers, students, parents and other members of the School community, employees should not expect privacy in this regard.

A reported or suspected breach of this policy is a serious matter and will be investigated by School management pursuant to the appropriate workplace procedure. The School reserves the right to use information that is expressly prohibited by this policy and which comes to School management's attention whether through monitoring or otherwise for disciplinary purposes.

Non-compliance by employees with any aspect of this policy may be subject to disciplinary action up to and including dismissal.

Presentation Girls' School, Maynooth

Success Criteria:

- Pupils have appropriate, supervised access to computer facilities and the internet
- Breaches, when they occur, are reported immediately, investigated with sensitivity and appropriate action taken.
- The computer system is easily maintained and is available for classwork as required i.e. downtime is kept to a minimum on all computers

Monitoring Procedures:

This policy will be monitored in the light of experience.

Review Procedures:

The policy will be reviewed periodically or as required.

This policy was approved by the Board of Management on

17th May 2022

Signed:

Doneann Ní Shingneá
Chairperson

School Website & Photograph Policy: 2017
Presentation Girls' Primary School, Maynooth, Co. Kildare.

The school has developed a website reflecting the activities which take place within the school community. Pupils will be given the opportunity to publish projects, artwork or class work on the World Wide Web once the content reflects and adheres to the guidelines of our Internet Use of Internet Policy. All content, photographs and video clips will be vetted by the Principal, class teachers and/or the ICT coordinator for approval prior to being loaded onto www.presgirlsmaynooth.ie

The content of the website will be regularly checked to ensure it does not compromise the safety of pupils and staff.

The publication of pupils' work will be coordinated by a teacher.

Photographs, audio and video clips will focus upon group activities. Content focusing on individual pupils will not be published on the school website without parental permission.

Personal pupil information including surname, home address and contact details will not be included on the website.

Photographs will not bear the pupils' name.

Pupils continue to own the copyright on any published work.

Parent's Consent for Web Publication of Work and Photographs

I agree that, my daughter's work may be published on the school Web site. I also agree that photographs that include my daughter may be published subject to the school rules that photographs will not clearly identify individuals and that names will not be used.

Signed: _____ (parent / guardian)

Pupil's name: _____ Date: _____.

Class: _____ Teacher: _____

Full policy is available on www.presgirlsmaynooth.ie

Presentation Girls' School, Maynooth

**Presentation Girls' School
Maynooth,
Co. Kildare.**

Dear Parent / Legal guardian,

Please review the attached school Internet Use Policy, sign and return this permission form to the Principal / class teacher.

Name of pupil: _____

Class / Year: _____

As the parent or legal guardian of the above named pupil, I have read the Internet Use Policy and grant permission for my daughter to access the Internet. I understand that Internet access is designed for educational purposes only. I also understand that every reasonable precaution has been taken by the school to provide for online safety but the school cannot be held responsible if pupils access unsuitable websites.

I will instruct my child regarding any restrictions set forth in the School Internet Use Policy. I will emphasise to my child the importance of following the rules for personal safety.

I hereby release the school and its personnel from any and all claims and damages of any nature arising from my child's use of, or inability to use, the school computer system, including, but not limited to claims that may arise from the unauthorized use of the system to purchase products or services.

Please sign and return to the class teacher / Principal:

Date: _____

I give/ do not give my daughter _____ permission to access sites on the Internet chosen by the teacher, for educational purposes only, during school time

Signed: _____.

Address: _____

Tel: _____

Appendix 1

Children's Rules for Online Safety

It is now very common for children to upload information on social networking sites. Caution is necessary to make sure that posts, images and videos are appropriate.

1. I will not give out personal information such as my address, telephone number, parents/guardians' work address/telephone number, or the name and location of my school without my parents/guardians' permission.
2. I will tell my parents/guardians right away if I come across any information that makes me feel uncomfortable.
3. I will never agree to get together with someone I "meet" online.
4. I will never send a person my picture.
5. I will not respond to any messages that are mean or in any way make me feel uncomfortable. It is not my fault if I get a message like that. If I do I will tell my parents/guardians right away.
6. I will talk with my parents/guardians so that we can set up rules for going online and using a mobile device. We will decide upon the time of day that I can be online, the length of time I can be online and appropriate areas for me to visit. I will not access other areas or break these rules without their permission.
7. I will not give out my passwords to anyone (even my best friends) other than my parents/guardians.
8. I will check with my parents/guardians before downloading or installing software or doing anything that could possibly hurt our computer or mobile device or jeopardize my family's privacy.
9. I will be a good online citizen and not do anything that hurts other people or is against the law.
10. I will help my parents/guardians understand how to have fun and learn things online and teach them things about the Internet, computers and other technology.

CYBERBULLYING

Cyberbullying occurs when bullying behavior is carried out through the use of ICT systems, such as, e-mail, mobile phones, Instant Messaging (IM), social networking websites, apps and other online technologies.

The most important feature of bullying is the intention to annoy, etc. However, we can also cause annoyance unintentionally.

Therefore, think before sending a message! Remember that the same message may be interpreted differently, depending on whether it was received as, for example, a text or as an oral message, by post, or as a tweet.

- **Don't respond in any shape or form to the provocation.** If someone bullies you, remember that your reaction is usually exactly what the bully wants. It gives him or her power over you. Who wants to empower a bully?
- **Don't retaliate.** Getting back at the bully turns you into one and reinforces the bully's behavior. Avoid a whole cycle of aggression.
- **Save the evidence.** In digital bullying, the harassing messages can usually be captured, saved, and shown to someone who can help.
- **Block the bully.** If the harassment's coming in the form of instant messages, texts, or profile comments, use preferences or privacy tools to block the person. If it's in chat, leave the "room." This may not end the problem, but you don't need harassment in your face all the time, and no reaction sometimes makes aggressors bored so they'll stop.
- **Reach out for help.** You deserve backup. Of course you know there are different kinds of help, from talking with a friend to seeing if there's a trusted adult who can help. It's usually good to involve a parent but - if you can't - a trusted adult can sometimes be helpful. Sometimes this can result in bullies getting the help they need to change their behavior.
- **Use reporting tools.** If the bullying took place via a social network, use that service's reporting or "abuse" tools - Stop, Block and Tell.
- **Be civil.** You're doing yourself a favour. Even if you don't like a person, it's a good idea to be decent and not sink to his or her level. Research shows that gossiping about and "trash talking" others increase your risk of being bullied.
- **Don't be a bully.** Even a few seconds of thinking about how another person might feel can put a big damper on aggression.
- **Be a friend, not a bystander.** Forwarding mean messages or just standing by and doing nothing empowers bullies and hurts victims even more. If you can, tell bullies to stop, or let them know bullying is not cool - it's cruel abuse of fellow human beings. If you can't stop the bully, at least try to help the victim and report the behaviour.

INTERNET SAFETY FOR YOU AND OUR PUPILS

The Internet can be a wonderful source of knowledge and entertainment for our children. They can use it to research school projects, communicate with other children, and play interactive games.

The internet has fast become a part of our everyday life. However, because it is not controlled by any organization, there are risks involved with its use. There are many ways that you, as a parent/guardian, can help protect your children from its dangers and ensure that your child's online experience is happy and productive.

Strategies for a responsible – and safer – online use

- Talk to your children about potential dangers on the internet - talk with them about your concerns, use filtering software, and keep a close eye on their activities.
- Make surfing the internet a family experience especially with younger children. Set family rules for its use such as when it can be used and for how long.
- Keep any internet device in a busy room in the house where you can see it.
- Ensure that your children never give personal information and remain anonymous at all times, never disclosing personal information, such as address, phone number, credit card numbers, school location, send pictures to strangers or meet with an online friend without permission.
- Encourage your children to talk to you about anything 'uncomfortable' they may find on the internet and to tell you about any communication or conversation that made them feel uncomfortable. Do not communicate with people they do not know.
- Never respond to a threatening email or message or open email from strangers – it may contain viruses that can harm a computer
- Share an email account with your child so you can monitor messages.
- Keep passwords private (except to parents)
- Bookmark children's favourite sites for easy access.
- Visit only age-appropriate sites. Check out the site before your child visits it. Know what features and what content exist and make sure they're suitable for your children.
- Be involved and have fun with your child. Start by showing interest in the sites they visit and the games they play and your job will be a lot easier when they start exploring these technologies more independently.

Being Savvy about the Internet and Online Protection Tools

Become computer savvy about the internet yourself and check out how your child uses this technology to interact with others on the internet. Check out www.internetsafety.ie for information regarding instant messaging, email, picture messaging, texting, social networking sites, chatrooms, net surfing, search engines, games consoles, online gaming, blogs etc. Online tools are available that will let you control your children's access to adult material and help protect them from Internet predators. No option is going to guarantee that they'll be kept away from 100% of the risks on the Internet. So it's important to be aware of your child's computer activities and educate them about online risks.

Many Internet service providers (ISPs) provide parent-control options to block certain material from coming into a computer. You can also get software that helps block access to certain sites based on a "bad site" list that your ISP creates. Filtering programs can block sites from coming in and restrict personal information from being sent online. Other programs can monitor and track online activity. Also, make sure they create a screen name to protect their real identity. Many sites use "cookies," devices that track specific information about the user, such as name, email address, and shopping preferences. Cookies can be disabled. Ask your Internet service provider for more information.

Resources for Parents and internet safety: www.kidshealth.org, www.internetsafety.ie, www.bewebsafe.net, www.scoilnet.ie, www.common sense media.org, www.webswise.ie, www.watchyourspace.ie

Presentation Girls' School, Maynooth

Social networking sites are for the use of over 13s and therefore we discourage their use. However we are aware that such sites are commonly used among the youth of today. They tend to create their own profiles, linking to their friends' profiles and sharing photos. If you permit your child to use such sites (e.g. Facebook, Instagram, Viber, SnapChat, Club Penguin, Stardoll), here are some suggestions to help your child be safe online:

- The internet is a public place and your child needs to be vigilant about who they communicate with online.
- Keep the internet device in a busy room in the house
- Learn how to use the technology yourself.
- Guard personal information online, even private sites are not 100% secure
- Think before they publish. Remember information and photographs which are published online are there forever
- They are not anonymous online –behaviour online can be traced and can be potentially damaging to themselves and others.
- Encourage them not to respond to communication which makes feel uncomfortable – tell a responsible adult about the situation immediately
- Set their profile to 'private'. That means only 'friends' can see their profile and send them messages.
- Online friends aren't always friends – be cautious when communicating with people online you don't know or trust.

What are the risks of children using social-networking websites?

- Bullying, intimidation and harassment
- Damaging their reputation and good name by their behaviour online
- Being approached by online predators, who may try to coax them into a real life meeting
- Giving out personal information online and not knowing who can see it
- Identity theft
- Publishing unsuitable photographs or videos of themselves online, e.g. with webcams. Once the images are online, they can be copied and circulated by other users
- Seeing inappropriate content (text, photographs, videos), including pornography, hate, racist and self-harm material
- Being influenced by the profiles of users who glamorise drinking, drugs, fast driving, or anti-social behaviour
- Spending too much time online and neglecting physical exercise or homework
- Breaking the law by posting copyrighted material online
- If you or your children ever come across content on the internet that you suspect to be illegal you can report it using the confidential www.hotline.ie service.