Stratford College
Co-educational Secondary School

Internet Acceptable Use Policy

Date of Commencement: 14th June 2023

Content

Scope of Policy: Whole School

Mission

The aim of this 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.

Please note: access to school platforms is access to our school environment and all rules, regulations and policies will apply while using them.

Rationale

Stratford College accepts that the use of tablet devices and smart phones is now an integral part of the lives of children and young people. While this is a positive development, concerns have been identified including some risks associated with the misuse, abuse and possible overuse of these devices and the various associated technologies. In light of 2018 findings from the World Health Organisation (WHO) regarding the detrimental effect of the use of Mobile Phones by teenagers on their long-term health, Stratford College will endeavour to protect students from the harmful use of these devices during school hours.

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 Therefore, if the school AUP is not adhered to this privilege will be withdrawn and appropriate sanctions – as outlined in the AUP – will be imposed.
It is envisaged that school and parent representatives will revise the AUP periodically.

The AUP is key to the Stratford College eLearning Policy and the Assessment for Learning (AfL) through eLearning Policy.

Aims:

To optimise teaching and learning for students
To reduce the possible distractions for students
To provide an environment free from threat or invasion of privacy
To discourage cyber bullying

To encourage face to face interaction and communication between students

Objectives

The school employs a number of strategies in order to maximise learning opportunities and reduce risks associated with the Internet. The ICT Co-ordinator(s) and subject teachers are responsible for informing their students of this policy. The strategies are as follows:

1. General
2. World Wide Web
3. Email, Social Media and Apps
4. School Website
5. Personal Devices
6. Legislation
7. Support Structures
8. Sanctions
9. User Policy for Mobile Devices

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 Acts 1988 to 2018 and General Data Protection Regulations (GDPR)
- Copyright and Related Rights Act 2000
- Child Trafficking and Pornography Act 1998 and Criminal Law (Sexual Offences) Act 2017
- Children First Act 2015
- Harassment, Harmful Communications and Related Offences Act 2020 (Coco's Law)

- Criminal Damage Act 1991

Support Structures

The school will inform students and parents of key support structures and organisations that deal with illegal material or harmful use of the Internet.

Policy Content

General Approach

When using the internet students, parents and staff are expected:

- To treat others with respect at all times.
- Not undertake any actions that may bring the school into disrepute.
- Respect the right to privacy of all other members of the school community.
- Respect copyright and acknowledge creators when using online content and resources.

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

- Filtering software and/or equivalent systems will be used in order to minimise the risk of exposure to inappropriate material.
- Uploading and downloading of non-approved software will not be permitted.
- The use of personal external digital storage media in school, requires school permission.
- Virus protection software will be used and updated on a regular basis.

- Internet use within school will always be supervised by a teacher.

This Acceptable Use Policy applies to students who have access to and are users of the internet in Stratford College.

- It also applies to members of staff, volunteers, parents, carers and others who access the internet in Stratford College.

Misuse of the internet may result in disciplinary action, including written warnings, withdrawal of access privileges, detention and, in extreme cases, suspension or expulsion. The school also reserves the right to report any illegal activities to the appropriate authorities.

Stratford College will deal with incidents that take place outside the school that impact on the wellbeing of students or staff under this policy and associated codes of behaviour and anti-bullying policies. In such cases Stratford College will, where known, inform parents/carers of incidents of inappropriate online behaviour that take place out of school and impose the appropriate sanctions.

Stratford College implements the following strategies on promoting safer use of the internet:

- Students will be provided with education in the area of internet safety as part of our implementation of the SPHE and other curriculum areas.
- Internet safety advice and support opportunities are provided to students in Stratford College through our [INDUCTION, PASTORAL CARE, ICT, PEER MENTORING programmes.
- Teachers will be provided with continuing professional development opportunities in the area of internet safety.
- Stratford College participates in Safer Internet Day activities to promote safer more effective use of the internet.

This policy and its implementation will be reviewed annually by the following stakeholders:

Board of Management, teaching staff, and support staff.

This policy has been developed by a working group including: Principal, Deputy Principal, teachers, students, parents/carers, and representatives of the Board of Management.

The school will monitor the impact of the policy using:

- Logs of reported incidents.
- Internal monitoring data for network activity.
- Surveys and/or questionnaires of students, parents, and teaching staff.

Should serious online safety incidents take place, Patricia Gordon should be informed.

The implementation of this Internet Acceptable Use policy will be monitored by the BOM and the Principal, Patricia Gordon.

Content Filtering

Stratford College has chosen to implement the following level on content filtering on the Schools Broadband Network:

PDST Level 6

This is the widest level of content filtering available. This level allows access to millions of websites including games and YouTube and allows access to personal websites category, and other similar types of websites, such as blogs. It allows access to websites belonging to the personal websites category and websites such as Facebook belonging to the Social Networking category.

This firewall is reinforced with an internal firewall that further filters out inappropriate content.

Students taking steps to by-pass the content filter by using proxy sites or other means may be subject to disciplinary action, including written warnings, withdrawal of access privileges, detention and, in extreme cases, suspension or expulsion.

Internet Use

Students will not copy information into assignments and fail to acknowledge the source (plagiarism and copyright infringement) or any use an Generative AI applications.

Students will not intentionally visit internet sites that contain obscene, illegal, hateful or otherwise objectionable materials.

Students will be encouraged to report accidental accessing of inappropriate materials in accordance with school procedures.

Students will report accidental accessing of inappropriate materials in school but outside the classroom to the Principal, Patricia Gordon.

Students and staff 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.

Students will use the Internet for educational purposes only.

Students will not download or view any material that is illegal, obscene, and defamatory or that is intended to annoy or intimidate another person.

Downloading by students of materials or images not relevant to their studies is in direct breach of the school's acceptable use policy.

Students will never disclose or publicise personal information or passwords.

Students will be aware that any usage of the internet and school's digital platform, including distributing or receiving information, school-related or personal, will be monitored.

Use of file sharing and torrent sites is never allowed.

Email and Messaging

Downloading by students of materials or images not relevant to their studies is not allowed.

The use of personal email accounts is not allowed at Stratford College.

- Students will use approved school email accounts.

- Students should not use school email accounts to register for online services such as social networking services, apps, and games.
- Students will use approved class email accounts only under supervision by or permission from a teacher.
- Students should be aware that email communications are monitored.

Students and staff will not send any material that is illegal, obscene, and defamatory or that is intended to annoy or intimidate another person.

Students and staff should immediately 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 and staff should avoid opening emails that appear suspicious. If in doubt, students should ask their teacher before opening emails from unknown senders.

Students and staff will not reveal their own or other people's personal details, such as addresses or telephone numbers or pictures.

Students will never arrange a face-to-face meeting with someone they only know through emails or the internet.

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 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.

All emails and opinions expressed in email are the responsibility of the author and do not reflect the opinion of the school.

Social Media and messaging services for Staff and Students

The internet provides a range of social media tools that allow us to interact and keep in touch. While recognising the benefits of these media for new opportunities for communication, this policy sets out the principles that members of your school community are expected to follow when using social media.

The principles set out in this policy are designed to help ensure that social media is used responsibly so that the confidentiality of students and other staff and the reputation of the school is protected.

This policy applies to personal websites such as social networking sites, blogs, micro blogs, chatrooms, forums, podcasts, and content sharing sites such as flickr and YouTube. The internet is a fast moving technology and it is impossible to cover all circumstances or emerging media.

The following statements apply to the use of messaging, blogging and video streaming services in Stratford College :

- Use of instant messaging services and apps is not allowed in Stratford College.

All members of the school community must not use social media, messaging services and the internet in any way to harass, impersonate, insult, abuse or defame others.

Staff and students must not discuss personal information about students, staff and other members of the Stratford College community on social media.

Staff and students must not use school email addresses for setting up personal social media accounts or to communicate through such media.

Staff and students must not engage in activities involving social media which might bring Stratford College into disrepute.

Staff and Students must not represent your personal views as those of bring Stratford College on any social medium.

Students will be provided with guidance on etiquette regarding social media.

Teachers can read further information about the use of Social Media and Electronic Communication here: https://www.teachingcouncil.ie/en/news-events/latest-news/2021/guidance-for-registered-teachers-about-the-use-of-social-media-and-electronic-communication.html

Personal Devices

After considerable consultation with staff, parents and the Board of Management Stratford College has decided that:

- **Only WIFI enabled digital devices are allowed in the classroom setting**
- These devices should not have software downloaded that allows them to circumvent the school WIFI system e.g. VPN. See Section titled: 'Inappropriate Activities'.
- Currently recommended devices are listed under 'Current Families' on the Stratford College website

- Junior students' phones must be kept in their phone away box. Senior students must keep their phones in their lockers throughout the school day. There will be a **No Visibility/No Carriage Rule in operation**. This means that it is not acceptable for students to have their phones on their person while in the school hall, in the corridors, the classroom or in evening study. If they are caught with their phones on their possession, they will have it confiscated. (please see our *Code of Behaviour and Discipline policy*).
    a. First Offence: it will be confiscated until the following day. It will be left at the office and it can be collected at end of the next day.
    b. Second Offence: If will be left in the office for three days and a parent must collect it.
    c. Third Offence: A week long confiscation will ensue, and a parent must collect it on the completion of the week. Parents/guardians are advised that all urgent communication for students should be directed through the school secretary.

- Digital device* usage in the classroom is teacher-led. Teachers will tell the students when to bring in their digital devices. They may not be needed for all classes or for every day.
- If a teacher has reason to believe that a student's device has been used to record
- Students sending nuisance text messages, or the unauthorized taking of images with a mobile phone/device camera, still or moving is in direct breach of the school's acceptable use policy, the school's Anti-Bullying Policy and the school's Code of Behaviour and Discipline Policy.
- It should be noted that it is a criminal offence to use a mobile phone/digital device to menace, harass, or offend another person. As such, the school may consider it appropriate to involve the Gardai in such incidents.
- **Right to search a device/view images**
- If a management has <u>reason to believe that a student's device contains images that are inappropriate, unauthorized or have been used to menace, harass, or offend</u> another person then they have the right to

ask to view the image. Management also has the right to search a student's device if they have reasonable grounds to believe that software has been downloaded that will allow VPN access.

- In accordance with our Child Protection Policy p 13, the student will be invited to have a guardian present or a teacher of their choice present. The search of their device will be carried out in the presence of the Principal or the Deputy principal or year head with another teacher to act as witness to the event. This occurs with the child's consent and does not breach their right to digital privacy.
- If a student refuses to provide access to the image/s concerned, then they may be prompted to do so by their parents but in circumstances where there is suspicion of a crime (see above point), the assistance of the Gardai will be sought.

Digital Learning Platforms (including video conferencing)

Stratford College digital learning platform is owned and managed by the school. This platform should enable two-way communication.

Students must only use their school email for accessing the school digital learning platform.

Only school devices should be used for the purposes of capturing and storing media.

All school-related media and data should be stored on the school's platform.

The use of digital platforms should be used in line with considerations set out in the school's data protection plan (GDPR).

Each user of the platform will be provided with their own unique login credentials.

Passwords for digital platforms and accounts should not be shared.

Personal email addresses should not be used when creating accounts on school digital platforms.

Prior acceptance from parents should be sought for student usage of the schools' digital learning platform.

Remote Learning

- Live/remote teaching and learning:

In order to ensure that the same level of courtesy we enjoy in the physical classroom is maintained online, we wish to share with you our expectations regarding online behaviour and ask that you share and discuss this protocol with your child.

- Be responsible
- Join the lesson on time.
- Immediately turn off the microphone when entering a meeting and turn it on when asked to do so.
- Send questions using the chat feature if requested by a teacher.
- Follow all expectations and guidelines set by your teacher.
- Be respectful in terms of participation, language, dress etc.
- Avoid any anti-social behaviour that would be deemed unacceptable in the classroom
- Use appropriate volume and academic language

- Be courteous and respectful of all teachers and students
- Your listening skills are really the focus of this type of learning. Do not interrupt.
- Wait your turn to be invited to speak (if you have been requested to mute sound)
- In Microsoft Teams, do not start a meeting, wait until your teacher starts the meeting. This is a kin to starting teaching the class without the teacher present.
- Respect others privacy. Recordings (photographs, voice and or video) are not permitted, they are in breach of our GDPR policy unless you are specifically requested to do so for a specific purpose as directed by your teacher.
- Please remain online until the teacher concludes the lesson.
- Please follow staff instructions to make this a positive learning experience for all involved.

Our Code of Behaviour which relates to acceptable online behaviour is fully outlined in our Acceptable User Policy (see appendix 1). Should a teacher deem a student's online behaviour to be unacceptable in the light of the above expectations, the teacher has the capacity to remove a student from the online class. We will ensure follow-up with an individual student in the aftermath of the lesson.

Images and Video

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.

At Stratford College students 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.

Written permission from parents or carers will be obtained before photographs of students are published on the school website.

Students must not 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 and absolutely prohibited behaviour, with serious consequences and sanctions for those involved. Sharing explicit images of other students automatically incurs suspension as a sanction.

Inappropriate Activities

- Promotion or conduct of illegal acts, e.g. under the child protection, obscenity, computer misuse and fraud legislation
- Misuse and fraud legislation
- Racist material
- Pornography
- Promotion of any kind of discrimination
- Promotion of racial or religious hatred
- Harmful content or threatening behaviour, including promotion of physical violence or mental harm

- Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute
- Using school systems to run a private business
- Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school
- Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions
- Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords)
- Creating or propagating computer viruses or other harmful files
- Carrying out sustained or instantaneous high volume network traffic (downloading / uploading files) that causes network congestion and hinders others in their use of the internet
- Child sexual abuse material
- Any other activity considered questionable

School Websites

Students will be given the opportunity to publish projects, artwork or school work on the internet in accordance with clear policies and approval processes regarding the content that can be loaded to the school's website.

Students will continue to own the copyright on any work published.

The website will be regularly checked to ensure that there is no content that compromises the safety, privacy, or reputation of students or staff.

Webpages allowing comments or user-generated content will be pre-moderated and checked frequently to ensure that they do not contain any inappropriate or offensive content.

The publication of student work will be coordinated by a teacher.

Personal student information including home address and contact details will not be published on Stratford College web pages.

Stratford College will avoid publishing the first name and last name of students in video or photograph captions published online.

The school will ensure that the image files are appropriately named and will not use students' names in image file names or ALT tags if published online.

Cyberbullying

This type of bullying is increasingly common and is continuously evolving. It is bullying carried out through the use of information and communication technologies such as text, social media, e-mail, messaging, apps, gaming sites, chat-rooms and other online technologies. Being the target of inappropriate or hurtful messages is the most common form of online bullying. As cyberbullying uses technology to perpetrate bullying behaviour and does not require face to face contact, cyber-bullying can occur at any time (day or night). Many forms of bullying can be facilitated through cyber-bullying. For example, a target may be sent homophobic text messages or pictures may be posted with negative comments about a persons sexuality, appearance etc.

Access to technology means that cyberbullying can happen around the clock and the students home may not even be a safe haven from such bullying. Students are increasingly communicating in ways that are often unknown to adults and free from supervision. The nature of these technologies means

digital content can be shared and seen by a very wide audience almost instantly and is almost impossible to delete permanently. While cyberbullying often takes place at home and at night, the impact can also be felt in school.

In accordance with the Anti-Bullying Procedures for Schools, Stratford College considers that a once-off offensive or hurtful public message, image or statement on a social network site or other public forum where that message, image or statement can be viewed and/or repeated by other people will be regarded as bullying behaviour.

When using the internet students, parents and staff are expected to treat others with respect at all times.

- Circulating, publishing or distributing (including on the internet) material associated with school activities including but not limited to material in relation to staff and students where such circulation undermines, humiliates or causes damage to another person is considered a serious breach of school discipline and may result in disciplinary action. Including written warnings, withdrawal of access privileges.
- As part of such disciplinary action the Board of Management reserves the right to suspend or expel a student or students where it considers the actions to warrant such sanctions.
- If a management has reason to believe that a student's device contains images that are inappropriate, unauthorized or have been used to menace, harass, or offend another person then they have **the right to ask to view the image**. In accordance with our Child Protection Policy, the student will be invited to have a guardian present or a teacher of their choice present. The search of their device will be carried out in the presence of the Principal or the Deputy principal or year head with another teacher to act as witness to the event. This occurs with the child's consent and does not breach their right to digital privacy.
- If a student refuses to provide access to the image/s concerned, then they may be prompted to do so by their parents but in circumstances where there is suspicion of a crime, the assistance of the Gardai will be sought. The school also reserves the right to report any illegal activities to the appropriate authorities, including An Garda Siochana.

The right to view an inappropriate, unauthorized image that may have been used to menace, harass, or offend another person is for the intended purposes:

1. Prevent bullying
2. Promote the health and safety of staff, students and visitors
3. Reduce the incidence of cyber crime
4. Support the Gardai in a bid to deter and detect crime
5. Assist in identifying, apprehending and prosecuting offenders
6. that school rules are implemented and respected and so the school can be properly managed.

Measures are taken by Stratford College to ensure that staff and students are aware that bullying is defined as unwanted negative behaviour, verbal, psychological or physical, conducted by an individual or group against another person (or persons) and which is repeated over time. This definition includes cyberbullying even when it happens outside the school or at night. In addition the Department of Education Anti-Bullying Procedures, 2013 defines cyberbullying as “placing a once-off offensive or hurtful public message, image or statement on a social network site or another public forum where that message, image or statement can be viewed and/or repeated by other people will be regarded as bullying behaviour.

The prevention of cyberbullying is an integral part of the anti-bullying policy of our school.

Acceptable User Form

Stratford College accepts that that the use of technology and electronic equipment including mobile phones is increasingly part of modern everyday life. However, we are also conscious of the negative impact that excessive access to mobile phones is having in on student and staff wellbeing and the potential damage they may contribute to normal social interaction. In light of the recent findings from the World Health Organisation (WHO) regarding the detrimental effect of the use of Mobile Phones by teenagers on their long-term

health, Stratford College will endeavour to protect students from the harmful use of these devices during school hours.

At the start of every academic year each student, parent and tutor must agree to adhere to the specifications of our Acceptable User Policy.

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 Acts 1988 to 2018 and General Data Protection Regulations (GDPR)
- Copyright and Related Rights Act 2000
- Child Trafficking and Pornography Act 1998 and Criminal Law (Sexual Offences) Act 2017
- Children First Act 2015
- Harassment, Harmful Communications and Related Offences Act 2020 (Coco's Law)
- Criminal Damage Act 1991

Support Structures

The school will inform students and parents of key support structures and organisations that deal with illegal material or harmful use of the Internet.

Sanctions

- Circulating, publishing or distributing (including on the internet) material associated with school activities including but not limited to material in relation to staff and students where such circulation undermines, humiliates or causes damage to another person is considered a serious breach of school discipline and may result in disciplinary action.

Including written warnings, withdrawal of access privileges.

- As part of such disciplinary action the Board of Management reserves the right to suspend or expel a student or students where it considers the actions to warrant such sanctions.
- If a management has reason to believe that a student's device contains images that are inappropriate, unauthorized or have been used to menace, harass, or offend another person then they have **the right to ask to view the image**. In accordance with our Child Protection Policy, the student will be invited to have a guardian present or a teacher of their choice present. The search of their device will be carried out in the presence of the Principal or the Deputy principal or year head with another teacher to act as witness to the event. This occurs with the child's consent and does not breach their right to digital privacy.
- If a student refuses to provide access to the image/s concerned, then they may be prompted to do so by their parents but in circumstances where there is suspicion of a crime, the assistance of the Gardai will be sought. The school also reserves the right to report any illegal activities to the appropriate authorities, including An Garda Siochana.

The right to view an inappropriate, unauthorized image that may have been used to menace, harass, or offend another person is for the intended purposes:

1. Prevent bullying
2. Promote the health and safety of staff, students and visitors
3. Reduce the incidence of cyber crime
4. Support the Gardai in a bit to deter and detect crime
5. Assist in identifying, apprehending and prosecuting offenders
6. that school rules are implemented and respected and so the school can be properly managed.

Misuse of the Internet and digital technologies are covered in our Code of Positive Behaviour Policy and our Anti-Bullying Policy.

Students when using their digital device in Stratford College must use the school WiFi connection and firewall as detailed in our Acceptable Computer User Policy. Please ensure that the digital device and associated peripherals

are named. Students are responsible for their own digital device when in school.

I agree to follow the school's Acceptable Use Policy on the use of the internet and digital technologies. I will use the internet and digital technologies in a responsible way and obey all the procedures outlined in the policy.

Please review the attached school Internet Acceptable Use Policy, and sign.

Student's Signature: _____

Parent/Guardian : _____

Date: _____

Roles and Responsibilities

Board of Management

- To ensure that the policy is developed and evaluated from time to time
- To approve the policy
- To consider reports from the Principal on the implementation of the policy

Principal, Deputy Principal and Class Tutors

- To ensure that students understand the AUP, sign it annually in their School Journal and comprehend the sanctions that can be imposed on them if they do not adhere to the policy
- To monitor the implementation of the policy

Subject Teachers

- To ensure that the use of internet access during class adheres to the AUP
- To apply the appropriate sanctions where a student transgresses the AUP

Pastoral Care Personnel (Class tutors, Guidance and Resource Personnel)

- To liaise with subject teachers especially in relation to Positive Health initiatives which are part of the school's Pastoral Care policy.

ICT co-ordinators

- To ensure that the appropriate filters and monitoring systems of internet access are in place at all times
- To monitor and update filters and monitoring systems as deemed appropriate

Success Criteria

- Internet access within the school is controlled to ensure a safe environment for students, teachers and staff
- Changes are made to filters and monitoring systems on an ongoing basis, as deemed appropriate
- Internet Safety awareness is embedded in all our teaching and learning
- A positive and respectful culture in terms of Internet Safety and mobile devices pervades the school
- Parents, students and teachers are satisfied with the effectiveness of this policy

Monitoring Procedures

- To ensure that the appropriate filters and monitoring systems of internet access are in place at all times
- To monitor and update filters and monitoring systems as deemed appropriate
- Logs and reports can be generated as required

Review Procedures

Ratified: Mr. Alan Green, School Manager	3rd May 2011
Updated: Ms. Siobhan Reynolds (DP) and Ms. Helen O'Kelly (Librarian)	18th March 2014
Updated: Ms. Catherine Conlon and Ms. Helen O'Kelly (ICT Co-ordinators)	12th May 2015
Submitted to the Board of Management for ratification	13th May 2015
Updated: Ms. Siobhan Reynolds (DP)	5th June 2019
Submitted to the Board of Management for ratification	6th June 2019
Revised by BOM	10 April 2020

Approved

Date: 14th June 2023

Mr John Rafter
Chair BOM

Ms Patricia Gordon
Secretary BOM

Appendix 1

ADVICE FOR APPROPRIATE ONLINE BEHAVIOUR

The Dos

- ☺ Do think carefully about how you present yourself when choosing a profile image. Your online reputation is important. Think also about the language you use even if used jokingly – what you say and do online lay down your digital footprint.
- ☺ Do trust your instincts. If something doesn't feel right, it probably isn't. If you find something online that you don't like, turn off the computer and tell an adult.
- ☺ Be careful about the images/comments you post on -line, as soon as it is posted, you have lost control over who will see it and how it will be used. Don't post anything that you wouldn't want everyone you know to see, including your parents and teachers.
- ☺ Do be careful with the personal information of others. Don't tag others in photos without their permission. Don't share their personal details and information with the world. Thay have a right to privacy and you have a responsibility to protect it.

The Don'ts

- ☹ Don't reply to abusive or upsetting messages. This is exactly what cyberbullies want. They want to know they've got to you and that you are worried or upset. They want to think that they are important by being able to get a reaction from you. Don't give them the satisfaction. Stay in control. Defriend them. Report them. If necessary, remove yourself from that social networking site.
- ☹ Don't assume everyone you meet online is who they claim to be. Information provided by users when they are registering is not checked. Anyone can create a fake profile.
- ☹ Don't post information that could be used to find you off-line. BE careful of posting photos with things like car registration plates or identifiable landmarks. Don't post messages about your daily routine. There are people out there who may piece together this information and use it against you.

Tips for Internet Safety:
Did you know that:

- ✓ Every photo and piece of information posted on a website becomes public property.
- ✓ Hackers can gain access to any system no matter how private you think it is.
- ✓ University admissions officers and prospective employers routinely enter names of students or job candidates into search engines
- ✓ Cyber bullying is increasing – gossip, is exchanged freely, causing great distress to the victims

Resources

https://www.webwise.ie/
https://support.office.com/en-ie/article/distance-learning-with-office-365-guidance-for-parents-and-guardians-89d514f9-bf5e-4374-a731-a75d38ddd588

https://www.youtube.com/watch?v=SemjM2fHV2Q&feature=youtu.be


The Parents Guide to Microsoft.pdf