# INTERNET ACCEPTABLE USE POLICY/CYBER SAFETY

## FOR

# ST. FRANCIS XAVIER SENIOR SCHOOL

## POLICY FORMATION

This policy was drafted by members of the staff of St. Francis Xavier Senior School. It was part of a whole school initiative on Internet Safety and was part of a leadership focused project and prepared by Niamh Greene, Aisling Brady, Shane Donaghy, Marianne Brennan and Stephen O'Leary.

This policy was ratified by the Board of Management on 28th September 2016.

## Introduction

St. Francis Xavier Senior School recognises that access to Information and Communication Technology (ICT) gives our students enhanced opportunities to learn, communicate and develop skills that will prepare them for many aspects of life. We believe in developing a modern learning environment rich in ICT resources to empower our children to make relevant and safe choices and to develop their personalised learning.

The aim of this Acceptable Use Policy is to ensure that pupils will benefit from opportunities offered by the school's Internet resources in a safe and effective manner. Internet use and access is considered a school resource and a privilege. This Acceptable Use Policy outlines the guidelines and behaviours that our students are expected to follow when using ICT. Consequently, if the school AUP is not adhered to this privilege may be withdrawn and appropriate sanctions will be imposed.

## Technologies at St. Francis Xavier School

St. Francis Xavier Senior school may provide students with Internet access, desktop computers, digital imaging equipment, laptop or tablet devices, video-conferencing capabilities, virtual learning environments, online collaboration capabilities, email and more. As new technologies emerge, St. Francis Xavier Senior School may provide access to them also. The policies outlined in this document are intended to cover all technologies in the school, not just those specifically mentioned.

## ICT Network

St. Francis Xavier ICT network is intended for educational purposes. All activity over the network may be monitored and retained. Access to online content via the network is restricted in accordance with the policies of the Department of Education and Skills, through its agency, the National Centre of Technology in Education. Students are expected to respect that the web filter is a safety precaution, and should not try to circumvent it when browsing the Web. If a site is blocked and a student believes it should not be, the student should ask his/her teacher to submit the site in question for review. Students are expected to follow the same rules of good behaviour online, as offline - these rules can be found in the Code of Behaviour and the Rules for Responsible Internet Use for pupils. Misuse of the school resources may result in disciplinary action. We make reasonable effort to ensure students' safety and security online, but will not be held accountable or liable for harm or damages that result from misuse of school technologies. Students are expected to alert his/her teacher immediately of any concerns for safety or security.

## St. Francis Xavier Senior School Strategy

The school will employ a number of strategies in order to maximise the learning opportunities of the children and reduce the risks associated with the internet.

### General

- Internet sessions will be supervised by a teacher.

- 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.
- Virus protection software will be used and updated on a regular basis.
- The use of CD-ROMs, USB sticks or memory cards in school requires a teacher's permission.
- Students will observe good 'Netiquette' (i.e etiquette on the Internet) at all times and will not undertake any actions that may bring the school into disrepute.

## World Wide Web

- Students will not visit Internet sites that contain obscene, illegal, hateful or otherwise objectionable materials.
- Students will take reasonable steps not to open or distribute infected files or programmes, and not to open files or programmes of unknown origin or untrusted origin.
- Students will use the Internet for educational purposes only.
- Students will be familiar with copyright issues relating to online learning.
- Students will never disclose or publicise personal information.
- Students will be aware that any usage, including distributing or receiving information, school-related or personal, may be monitored for unusual activity for security and/or network management reasons.

## Email and Online Collaboration

- St. Francis Xavier Senior School may provide students with an email account for the purpose of school related communication.
- Email accounts should be used with care. Email usage may be monitored and archived.
- St. Francis Xavier School recognises that online collaboration can have an educational value and may provide students access to many online tools that allow communication, information sharing, and messaging among students.
- Students are expected to communicate with the same appropriate, safe, mindful and courteous conduct online as offline.
- Students will note that sending and receiving email attachments at school are subject to the permission from the teacher
- Students will not send or receive any material that is illegal, obscene, defamatory or that is intended to annoy or hurt another person.
- Students will not reveal their own or other peoples personal details, such as addresses or phone numbers or photographs.
- Students will never arrange a face to face meeting with someone they met online.

## Internet Chat

- Students will only have access to chat rooms, discussion forums or other electronic communication forums that have been approved by the school.
- Chat rooms, discussion forums and other electronic communication forums will only be used for educational purposes and will always be supervised.
- Usernames will be used to avoid disclosure of identity.
- Face to face meetings with someone organised via the Internet is forbidden

## Mobile Devices

St. Francis Xavier Senior School does not at present permit students to use personally owned devices at school. Students who need to have a mobile phone in their possession need to request permission from the school and have it registered. Mobile phone permission forms are available from the office. Permission is granted on the basis that there is a significant need for the student to have the mobile phone in school. Mobile phones must be switched off for the entire school day and while on the school premises. Students who are found in possession of unregistered phones will be disciplined and their mobile phone confiscated.

## St. Francis Xavier Senior School Website

Our website is located at http://www.sfxns.ie/seniorschool/ St. Francis Xavier Senior School is committed to using our website in order to promote our school, showcase student work and to provide information for our students, their parents/guardians and the general public.

- Students may be given the opportunity to publish projects, artwork or school work on the World Wide Web.
- The publication of student work will be overseen by a teacher.
- Pupils work may appear in an educational context on Web pages with a copyright notice prohibiting the copying of such work without express permission.
- The creation and publishing of photographs, audio and video clips will focus on educational activities.
- Personal information including home address and contact details will be omitted from school web pages.
- St. Francis Xavier Senior School will continue to own copyright on any work it publishes.

## Netiquette

**(1) Netiquette** may be defined as appropriate social behaviour over computer networks and in particular in the online environment. To this end:

- Students should always use the Internet, network resources, and online sites in a courteous and respectful manner.
- Students should also recognise that not all online content is correct and appropriate and should use trusted sources when conducting research online.
- Students should never post anything online that they wouldn't wish their grandparents, parents/guardians, teachers, future colleges or employers to see.

Students should be mindful of the fact that once something is online, it is out there-and can sometimes be shared and spread in ways students never intended.

### (2) Plagiarism

Students should not plagiarise content (copy or use as your own without citing the original creator) including words or images, from the internet.

### (3) Cyberbullying ( this section should be read in conjunction with other school policies)

St. Francis Xavier Senior School is committed to adhering to the ***Anti-bullying Procedures for Primary and Post-Primary Schools (2013)***

2.1.1 ...where bullying is defined as 'unwanted negative behaviour, verbal, psychological or physical conducted by an individual or a group against another person (or persons) and which is repeated over time.'

2.1.2The following types of bullying behaviour are included in this non-exhaustive definition:

(i) deliberate exclusion, malicious gossip and other forms of related bullying;

(ii) cyber-bullying; and

(iii) identity- based bullying such as homophobic bullying, bullying based on a person's membership of the Traveller Community and bullying of those with disabilities or special needs.

2.1.3 In addition ..........placing a once-off offensive or hurtful message , image or statement on a social network site or other public forum where that message, image or statement can viewed and/or repeated by other people will be regarded as bullying behaviour.

*****Cyber-bullying will not be tolerated in St. Francis Xavier Senior School*****

**Note to students:**

- ❖ Don't be mean- don't send emails or post comments or photos with the intent of scarring, hurting, annoying or intimidating someone else.

- Engaging in any online activities intended to harm (physically, mentally or emotionally) another person, will result in severe disciplinary action and immediate loss of privileges.
- St. Francis Xavier Senior School will support students, teachers and parents in dealing with cyberbullying.
- St. Francis Xavier is committed to the *Child protection Procedures for Primary and Post Primary Schools (Circular 0065/2011) the Department of Education and Skills, the Department of Children and Youth affairs, the Department of Justice and Equality and the Health Service Executive*

## Addendum - Social Media

St Francis Xavier Senior School recognises and appreciates the important contribution that social media has made to enhance communication and interaction in the digital age in which we live. As a school community we believe that this resource - if harnessed constructively - can be used to change and enhance the way we teach, learn and interact with one another. We acknowledge the influence social media has on communication and interaction allowing us to share information and opinions with a broad audience. We are committed to developing the technological and communicative skills of our pupils by encouraging responsible and safe use of the internet. We believe this to be the shared responsibility of the parents, teachers, pupils and wider school community.

### Definition

Social media is an umbrella term used to describe websites or internet applications that allow people to interact with each other, by sharing information, opinions, knowledge and interests. In recent questionnaires distributed to our pupils, websites and apps such as Facebook, Snapchat, Instagram, Flipogram, Whatsapp, Oovoo, Viber, Kik and Skype are a few examples of what media our children are using. Social media also include services such as bloggs, video and audio podcasts, wikis, message boards, photo document and video sharing websites such as YouTube and micro blogging services such as Twitter. This definition is not exhaustive as technology is constantly developing new ways of communicating.

### Rationale

St. Francis Xavier Senior School acknowledges the positive role the internet plays in the education of our pupils, however, as a school we wish to alert pupils to the scope for irresponsible and inappropriate use of Social Media sites which can lead to bullying, harassment and access to inappropriate or illegal material while online or where victims can be subjected to inappropriate and unsolicited comments. The staff of St. Francis Xavier School acknowledge that this negative commentary is not confined to the classroom but extends into the wider community often having damaging consequences for victims. We recognise that this new virtual playground is often unsupervised and unregulated. The devising of this policy is a response to this new reality, calling us as a school community to come together and teach responsible internet use.

## Scope

This policy applies to the entire school community-management, teachers, staff, pupils and parents/guardians. Due to the diverse nature of access to Social Media, this policy relates to all such interactions both during and outside of normal school hours and includes the use of school and personal devices.

## Aims of this policy:

- to produce a set of strategies for students that will enable them to use Social Media safely and responsibly.
- to help protect the integrity and good name of all members of the school community from online abuse
- to outline behaviours which are unacceptable and the consequences for engaging in these.
- to outline procedures for school community members who find themselves the victims of inappropriate social media behaviour.
- to establish the role of teachers and parents in encouraging safer internet use and reporting of incidents.

## Roles and Responsibilities

1. The Board of Management will approve the policy and ensure its development and evaluation.
2. The Principal and Deputy Principal will be responsible for the dissemination of the policy; the application of sanctions; and together with the Parents' Association schedule workshops and guest speakers on this topic.
3. The Internet Safety Committee will outline unacceptable uses of Social Media to students.
4. Class teachers and parents will advise children on safe internet use.
5. Children and parents will be expected to read, understand and sign an Internet Safety Contract.
6. Strategies to ensure online safety will be taught as part of an SPHE Anti-bullying programme.
7. Teachers will report incidents of online bullying and be mindful of the obligations under Child Protection Guidelines.
8. The school community will provide support for students who have been victims of online bullying

## Principles of Safe and Responsible use of Social Media

In the social media world the line between private and public is not well defined nor is the line between personal and professional.

- Be selective about what you share. Everything happens in front of a vast, invisible and often anonymous audience. Once something is out there, it doesn't disappear as it can be copied and forwarded easily and quickly. Everything leaves a digital footprint. You should never post personal details such as your phone number, email address or home address.
- Be selective with friends. Be careful who you make friends with online. In general, it is better to restrict friends to people you know and trust. Talk to parents before adding friends you are not sure of.
- Never post your location. Facebook lets users post their location on every post. Children should not do this for safety and privacy reasons.
- Use strict privacy settings. Review all of the options on your privacy settings page. Many sites default settings tend to keep information public until a user makes it private.
- If your profile is linked to your mobile phone, you should use the websites privacy settings to ensure your phone numbers not visible.
- Chat/VoIP services (These allow for communication that maybe typed or spoken with or without webcam access). You should only communicate with people you trust and remember that others may be able to view all aspects of communication.

## Communication between Pupils/Parents/School Staff

1. Communication between pupils and staff, by whatever method, should take place within clear explicit professional boundaries. This includes the wider use of technology such as mobile phones, text messaging, emails, digital cameras, videos, web-cams, websites and blogs.

2. Teachers can be contacted via the school phone number. Staff should not give their personal mobile numbers or personal email addresses to pupils or parents.

3. Staff should not request, nor respond to, any personal contact made by a pupil to them on a social media site and should inform school management immediately of same.

4. Members of the school community need to ensure that when they are communicating about others, even outside school, that they give due regard to the potential consequences of such comments. Making comments or allegations on social networking sites about others connected with the school could result in formal action being taken against them. This includes the uploading of photographs that might bring a person, persons or the school into disrepute.

## Guidelines for staff on the use of Social Media Sites

### Personal use of Social Media

The use of Social Media sites by staff is governed by the recently published Code of Professional Conduct from the Teaching Council.

Teachers shall (Teaching Council)

- Communicate effectively with pupils, colleagues, parents, school management and others in a manner that is professional, collaborative and supportive, and based on trust and respect.
- Ensure that any communication with pupils/ students, colleagues, parents and school management is appropriate, including communication via electronic media, such as email, texting and social networking sites.
- Ensure that they do not access, download or otherwise have in their possession while engaged in school activities, inappropriate or illegal materials/images in electronic or other format.

Staff are encouraged to use the privacy settings on social media sites/apps and to keep updated on developments on privacy restrictions.

Staff are expected to exercise sound judgement and maintain the highest professional standards while using social media in the school.

## Unacceptable uses of Social Media sites and their consequences

Users are responsible for their own behaviour when communicating with social media and will be held accountable for the content of their communications that they post on social media locations.

### Unacceptable use of Social Media

- Sending or posting discriminatory, harassing, negative comments, threatening messages or images that may cause harm to any member of the school community.
- Forwarding, 'Liking' or commenting on material that is likely to cause offence or hurt to a third party.
- Sending or posting messages or material that could damage the school's image or a person's reputation.
- Creating a fake profile that impersonates any other member of the school community.
- Sending or posting material that is confidential to the school.
- Participating in the viewing or exchanging of inappropriate images or obscene material.

While all cases involving the inappropriate use of social media will be dealt with on an individual basis, the school and its Board of Management considers the above to be serious breaches of our Code of Behaviour. Disciplinary action will be taken in the case of inappropriate use of social media tools.

## Sanctions for Policy Infringements

Infringements of this policy may have disciplinary repercussions, including (but not exclusively):

- Suspension of computer privileges in school
- Confiscation of devices if found on school grounds or on school related activities
- Notification to parents /(misdemeanour/yellow card)
- Suspension from school and school- related activities
- Exclusion
- Legal action and/or prosecution

## Monitoring and Review

This policy will be monitored by the steering committee on Internet Safety In conjunction with the Principal and the Board of Management. Reviews will be undertaken as deemed necessary. A major review will be undertaken three years subsequent to the date of implementation.

Ratified by the Board of Management on 28th September 2016.

*John Mitchell* (Chairperson)

On behalf of the Board of Management.

## APPENDIX 1

# Internet Safety Contract- Rules for Responsible Internet Use

These rules will help to keep us safe and help us be fair to others. Please read through these rules carefully with your child.

**I will**

- I will only use ICT in school for school purposes. I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe.
- I will follow the same guidelines for respectful, responsible behaviour online that I am expected to follow offline.
- I will alert a teacher if I see threatening/bullying, inappropriate or harmful content (images, messages or posts) online.
- I will be cautious to protect the safety of myself of others.
- I will help to protect the security of the schools resources.
- I will only open/delete my own files. I will not access other people's files.
- I will ask the permission of the teacher before using the internet.
- I will only send e-mail messages, using a class or school e-mail address with my teacher's approval. The messages I send will be polite and responsible.
- I will only open e-mail attachments from people I know, or who my teacher has approved.
- I will treat my username and password like my toothbrush – I will not share it nor will I use any other person's username or password.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

**I will not**

- I will not engage in making negative comments about others, forwarding comments or 'liking' negative comments or images of others in the school community.
- I will not engage in cyber-bullying, harassment, or disrespectful conduct towards others in school or out of school.
- I will not agree to meet someone I met online in real life.
- I will not use language online that would be unacceptable in the classroom.
- I will not deliberately look for, save or send anything that could be inappropriate or offensive. If I accidentally find anything like this, I will close the screen and tell a teacher/parent **immediately** as this will protect other children and myself.
- I will not give my full name, my home address or telephone number nor those of any others online.

- I will not bring in mobile devices such as phones that are unregistered, cameras, ipods, memory sticks, software or CDs from outside school to use in school or take them on school trips.

**I understand**

- I understand the school can check my computer files and the Internet sites I visit, and that my parent/guardian will be contacted if a member of staff is concerned about my safety.
- I understand that the school also has the right to take action against me if I am involved in incidents of inappropriate behaviour when I am out of school and where they involve my membership of the school community (for example Cyber-bullying, use of images or personal information).
- I understand that if I fail to comply with the Rules for Responsible Internet Use Agreement. I will be subject to disciplinary action.

**Child:** As a school user of the Internet, I have read the Rules for Responsible Internet use with my parents/guardians, and I agree to comply with them and behave in a responsible way when online at home and at school.

**Child's name (print):...........................................................................**

**Child's signature: ...............................................................................**

**Parent:** I have read the Rules for Responsible Internet use with my child. I understand that some material found on the internet maybe objectionable and I accept responsibility for setting standards for my child when selecting, sharing and exploring information on the internet.

**Parent's name (print):.........................................................................**

**Parent's signature...............................................................................**

## APPENDIX 2

# Advice for Parents on Internet Safety

- Be informed about your child's internet use so that going online is a positive experience for you and your child.
- Discover the internet together, **parental guidance** on internet use places your child at an advantage and develops a positive attitude to internet exploration and makes it easier to share positive and negative experiences in the future
- Agree with your child rules for internet use in your home
- Discuss an acceptable length of time for your child to use the internet, spending hours alone and unsupervised on the internet is not good for your child.
- Agree on how to treat personal information - encourage your child never to give out personal name, address, username, password or location. Check your child's privacy settings and location settings.
- When gaming online, encourage your child to use a nickname for their password. Check out the content of their games. Children in primary school should not be playing games that have an age rating of 18 years. Check out the games your children are playing, sit down and play with them. Call of *Duty Black Ops* and *Grand Theft Auto* or other 15, 18 age-rated games are deemed unsuitable for primary school children.
- Discuss how to behave towards others when gaming, chatting, e-mailing and messaging. Encourage your child be responsible for what they post online. Encourage them to own up if they are wrong. We are all learning about responsible internet use.
- Teach your child that all comments posted online can be traced to the IP address of their internet device-nothing is anonymous.
- Social media sites like *Viber, Whatsapp, Snapchat, Facebook, Twitter, Kik , Oovoo* etc have an age rating of 13. Primary school children should not to be using them.
- Be aware that some social media sites are set up by unknown groups with different agendas. Your child may be at risk.
- Teach your child that Skype, Facetime and other webcam sites are for family and closely selected friends.
- Teach your child that posting a photograph online has ramifications, the image is there forever, can be passed on and can be exploited. Once the digital image is online, it is out of your hands. A photograph doesn't disappear forever after a number of seconds.
- Be careful about allowing your child free access to *Youtube*. They can gain access to a lot of inappropriate material. Dangerous challenges that are put up on *Youtube* encourage children to copy them.
- Be aware if you child has posted images or videos of themselves on Youtube or elsewhere online. The Internet has a vast audience. Making a video and posting it on Youtube is dangerous.
- Agree on what types of sites and activities are OK in your family. Be involved with the sites your child is engaged with, know how they work.

- Talk about the risks associated with meeting online ‘friends’ in person. Teach your child not to meet anyone, stranger or otherwise, without your permission.

- Teach your child about **evaluating information** and being critically aware of information found online.

- Report online material you may consider **illegal** to the appropriate authorities.

- Encourage **respect for others** and help stamp out cyber-bullying. Encourage your children to **REPORT, BLOCK** and **TELL** if they are being cyberbullied. **Do not retaliate.** Record everything- keep all text messages, keep a note of calls, screen shot images and messages.

    - Teach your child to protect their phone with a password and encourage them to share the password with you. Starting this practice at a young age can help you gain access to your child’s virtual world. Download a child-friendly search engine to filter age appropriate material for your child.

    - Let your children show you what they like to do online, be aware of **how** they are using the internet.

    - Do not let your child have their internet device in their bedroom. Do not let them use it late at night or unsupervised. Internet use should be in a **common space** to encourage openness and to enable monitoring. There should be restrictions on time usage.

    - Use **filtering software** designed to help parents limit the web-sites children can access.

**N.B (If you are completely unsure when it comes to the Internet, gaming, social media and general technology, be open, seek help from the school or friends - We are all learning!)**

***<u>Internet safety sites and links:</u>***

*www.webwise.ie*

*www.esafety.ie*

*www.netsmatz.org*

*www.digizen.org*

*www.thinkuknow.co.uk*

**APPENDIX 3**

## Acceptable Internet Use and E-Safety Permission Form

**Child:** As a school user of the Internet, I have read the Rules for Responsible Internet use with my parents/guardians, and I agree to comply with them and behave in a responsible way.

**Child's name (print) :.........................................................................**

**Child's signature: ........................................................................**

**Parent:** As the parent or legal guardian of the child signing above, I grant permission for my child to use the internet. I have read the Rules for Responsible Internet use with my child. I understand that some material found on the internet maybe objectionable and accept responsibility for setting standards for my child when selecting, sharing and exploring information on the internet.

**Parent's name (print):......................................................................**

**Parent's signature.........................................................................**