INTERNET SAFETY: ACCEPTABLE USE POLICY

St. Patrick's Boys' N.S.
Dublin Road, Limerick Roll no: 16443A

Contents

Overview....2

The Policy Review Team....2

School Strategy....2

Children's Use of the Internet....3

1. World Wide Web....3

2. Internet Chat / Social Networking / Instant Messaging (IM)....3

5. School website (www.stpatricksboysns.com) & Facebook page (https://www.facebook.com/stpatricksboysns/)....4

6. Student Laptops....5

7. Personal Devices....5

8. Cyberbullying Understanding Cyber Bullying:....5

Legislation....6

Sanctions....6

Other Relevant Policies....7

Support Structures....7

Appendix 1 (contained in the parental permission form)....8

Appendix 2....9

Appendix 3 Tusla Online Safety Appendix 7 13

Appendix 4

Addendum to Children First: National Guidance for the Protection and Welfare of Children....18

Overview

This Acceptable User Policy (AUP) relates to the use of the internet by students within the school.

The Policy Review Team

The AUP was revised by the staff in the school. Mrs Tierney is currently the ICT coordinator.

It has been read and ratified by the Board of Management and representatives of the parents and teachers within the school. It is envisaged that school and parent representatives will revise the AUP as necessary. Before signing, the AUP should be read carefully to indicate that the conditions of use are accepted and understood.

The aim of the AUP is to ensure that pupils will benefit from learning opportunities offered by the school's internet resources in a safe and effective manner. 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 Therefore, if the school AUP is not adhered to, this privilege will be withdrawn and appropriate sanctions, outlined in the AUP, will be imposed.

School Strategy

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

The strategies are as follows:

1. Where children have access to the internet in school, it will occur under the supervision of a teacher. Content will be subject to the restrictions of the Schools Broadband Internet Policy, which operates an automated web-filtering function of the PDST Technology in Education. The purpose of content filtering is to ensure (in so far as possible) that inappropriate websites and content are not accessible from within schools. - See more at: http://www.pdsttechnologyineducation.ie. Any requests for modification of the filtering provision that is in place for St. Patrick's Boys' National School may only be submitted in consultation with the Principal.
2. The school will regularly monitor internet usage (see Children's Use of the Internet below).
3. Children will not have access to passwords or administrator accounts.
4. Uploading and downloading of non-approved software will not be permitted.
5. Virus protection software will be used and updated on a regular basis.
6. If a teacher wishes to integrate a web page into a lesson, that page must be previewed/evaluated prior to its classroom usage, for inappropriate advertising content, imagery, and text.
7. The downloading of software, from storage devices or online sources, must be preapproved by the ICT Coordinator.

Children's Use of the Internet

1. World Wide Web

Children who have access to the internet will do so in adherence to the above strategies.

1. Before students are allowed to make use of the school's internet facility, all Parents/Guardians will be required to complete a Permission Form. Permission forms will be sent home via Aladdin to families in September of each year and the school's database will be updated accordingly.
2. Websites that the children use in school will be previewed by their teacher before use and subject to the filters operated by the Oide and Schools Broadband programme.
3. Teachers and students will be familiar with copyright issues relating to online learning.
4. Children will never disclose or publicise personal information.
5. If students see a message, comment, image, or anything else online that makes them concerned for their personal safety, they must bring it to the immediate attention of
    i. a teacher if they are at school
    ii. a parent / guardian if they are at home

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

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

3. Google Drive

1. When using Google Classroom and the Gsuite Apps, students will use approved class gmail accounts under supervision of a teacher or parent/guardian.
2. They will not have email accounts but will have access to google drive and classroom
3. Students will not send or receive any material that is illegal, obscene, defamatory, or that is intended to annoy or intimidate another person.
4. Students will not reveal their own or other people's personal details, such as addresses or telephone numbers or pictures.
5. Students will note that sharing documents is subject to permission from their teacher.
6. Children will observe good "netiquette" (internet etiquette) at all times and will not undertake any actions that may bring the school into disrepute.

4. **Distance Learning**

1. In circumstances where teaching cannot be conducted on the school premises, teachers may use Class Dojo, Google Classroom, Google Meet, Zoom, Padlet or other platforms approved by the school as platforms (the "Online Platforms") to assist with remote teaching where necessary.

2. The school has signed up to the terms of service of the Online Platforms in use by the school.

3. The School has enabled the most up to date security and privacy features which these Online Platforms provide.

4. In the case of Google Classroom and Google Meet, parents/guardians must grant access to their child to have a school Gmail address such as 23.pupilname@stpatricksboysns.com (Parental Permssions)

5. Parents/guardians will be provided with the password and will be expected to monitor their child's use of the Gmail address and Online Platforms.

6. If teachers are using Zoom/Google Meets, consent will be sought from parents/guardians prior to starting.

7. Parents/guardians must also agree to monitor their child's participation in any such lessons conducted on the Online Platforms as per our parents' information note (Appendix 2) and consent forms (Appendix 1)

5. School website (www.stpatricksboysns.com) & Facebook/Instagram (https://www.facebook.com/stpatricksboysns/, @StPatricksbnslk

The school website is used to celebrate the success stories and great achievements of our students as well as to publicize school events and activities and is evolving all the time. The school's Facebook/Instagram/Twitter (social media) pages are used to publicise school events, activities and at times, pupils' work.

Website

1. The school website and social media are administered by the ICT Team.
2. Only administrators of the social media pages will be able to tag photographs. No child's photograph will be tagged.
3. Children will be given the opportunity to publish projects, artwork, and school work on the school website.
4. The publication of student work will be coordinated by the teacher and/or ICT team.
5. Children will continue to own the copyright on any works published.
6. The copying of such content is prohibited without express written permission from the relevant child and his/her parent(s)/guardian(s).
7. Photographs /Videos/ other multimedia may be used on the school website and Facebook page to complement text content.
    a. Photographs of the children will only be displayed online through our various platforms with explicit consent from parents/guardians via Aladdin Permissions. .
    b. The school website will only publish the forenames of individuals in a photograph.
    c. Should an individual's full name be used at any stage, verbal permission will be sought from parents/guardians.
    d. No child's photograph shall be displayed if he is pictured on his own.
    e. Only Facebook page administrators can tag photos posted on it.

Children's Use of the Internet

1. World Wide Web

Children who have access to the internet will do so in adherence to the above strategies.

1. Before students are allowed to make use of the school's internet facility, all Parents/Guardians will be required to complete a Permission Form. Permission forms will be sent home via Aladdin to families in September of each year and the school's database will be updated accordingly.
2. Websites that the children use in school will be previewed by their teacher before use and subject to the filters operated by the Oide and Schools Broadband programme.
3. Teachers and students will be familiar with copyright issues relating to online learning.
4. Children will never disclose or publicise personal information.
5. If students see a message, comment, image, or anything else online that makes them concerned for their personal safety, they must bring it to the immediate attention of
    i. a teacher if they are at school
    ii. a parent / guardian if they are at home

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

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

3. Google Drive

1. When using Google Classroom and the Gsuite Apps, students will use approved class gmail accounts under supervision of a teacher or parent/guardian.
2. They will not have email accounts but will have access to google drive and classroom
3. Students will not send or receive any material that is illegal, obscene, defamatory, or that is intended to annoy or intimidate another person.
4. Students will not reveal their own or other people's personal details, such as addresses or telephone numbers or pictures.
5. Students will note that sharing documents is subject to permission from their teacher.
6. Children will observe good "netiquette" (internet etiquette) at all times and will not undertake any actions that may bring the school into disrepute.

4. **Distance Learning**

1. In circumstances where teaching cannot be conducted on the school premises, teachers may use Class Dojo, Google Classroom, Google Meet, Zoom, Padlet or other platforms approved by the school as platforms (the "Online Platforms") to assist with remote teaching where necessary.

6. Instant messaging (IM) – unpleasant messages sent while children conduct real-time conversations online using MSM (Microsoft Messenger), Yahoo Chat or similar tools.
7. Bullying via websites – use of defamatory blogs (web logs), personal websites, gaming websites, apps, online personal 'own web space' sites such as You Tube, Facebook, Ask.fm, Twitter, Snapchat, among others, emerging technologies and all electronic means.

Procedures for preventing Cyber Bullying:

1. Staff, pupils, parents, and Board of Management (BOM) are made aware of issues surrounding cyber bullying.
2. Pupils and parents will be urged to report all incidents of cyber bullying to the school.
3. Staff CDP (Continuous Professional Development) will assist in learning about current technologies.
4. Webwise.ie is used as a resource to teacher children and parents about the dangers present online.
5. Pupils will learn about cyber bullying through Social, Personal and Health Education (SPHE), Assemblies, Friendship Week activities and other curriculum projects.
6. Pupils, parents, and staff will be involved in reviewing and revising this policy as school procedure.
7. All reports of cyber-bullying will be noted and investigated, in accordance with the school's Anti-Bullying, Mobile Phone, Child Protection, and Code of Behaviour Policies, where applicable.
8. The school will engage a speaker Community Guard to facilitate a workshop on Internet Safety for 5th & 6th Classes and mark Safer Internet Day (SID) annually.
9. Procedures in the school's Anti-Bullying and Child Protection policies shall apply. Incidents of cyberbullying will be addressed in the context of the school's Anti-Bullying, Mobile Phone, and Code of Behaviour Policies, where applicable.

Legislation

- Data Protection Act 2018
- Child Trafficking and Pornography Act 1998 - Interception Act 1993 - Video recordings Act 1989
- Children First 2017

Sanctions

Misuse of the internet may result in disciplinary action, including written warnings, withdrawal of access privileges and, in extreme cases, suspension or expulsion. Sanctions issued will be done so in accordance

with the school's Anti-Bullying Policy and Code of Behaviour Policy. The school also reserves the right to report any illegal activities to the appropriate authorities.

Other Relevant Policies

- Child Safeguarding
- Mobile Phone Policy
- Anti-Bullying Policy
- ICT Policy

Support Structures

Websites offering support and advice in the area of Internet Safety are listed here

· NCTE - http://www.ncte.ie/InternetSafety/

· Webwise - http://www.webwise.ie/

· Make IT Secure - http://makeitsecure.ie

· Safe Internet - http://www.saferinternet.org/ww/en/pub/insafe/

Signed: _____
(Chairperson of Board of Management)

Signed: _____
(Principal)

Date: 24/1/24

Date: 24/1/24

Appendix 1 (contained in the parental permission form)

Internet:

Parent/Guardian

As the parent or legal guardian of the above pupil, I have read the Acceptable Use Policy and grant permission for my son or daughter or the child in my care to access the Internet. I understand that Internet access is intended for educational purposes. 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 accept the above paragraph ☐ I do not accept the above paragraph ☐

(Please tick as appropriate)

Social Media

In relation to the school website and Facebook/Instagram page. I accept that, if the school considers it appropriate, my child's photograph and/or schoolwork may be chosen for inclusion on the website/Facebook page. Best practice as stated in our 'Acceptable Internet Use Policy' will always be followed. Usually children will only be pictured at a distance and in groups. Do you agree to the school using your child's image in this way? I understand and accept the terms of the Acceptable Use Policy relating to publishing children's work on the school website/Facebook page.

I accept the above paragraph ☐ I do not accept the above paragraph ☐

(Please tick as appropriate)

As the parent or legal guardian of the above pupil, I have read the Acceptable Use Policy and grant permission for my son or the child in my care to access one-to-one video calls using the agreed platforms (appendix 2). I understand that this is intended for educational purposes. I also understand that every reasonable precaution has been taken by the school to provide for online safety and accept my responsibility in providing adequate supervision for such activities.

I accept the above paragraph ☐ I do not accept the above paragraph ☐

(Please tick as appropriate)

Name of child(ren): _____

Signature: _____

Date: _____

Appendix 2

Information Note for Parents/Guardians and pupils regarding the use of Video/Phone Calls and Video/Audio Recordings in Online Teaching and Learning and Learner Contact using Zoom/Google Meet

As part of distance learning during this school closure, St Patrick's Boys' National School has decided that it may be necessary for our teachers/special needs assistants to communicate with your son through the use of video calling, and to use video or audio recordings as part of the teaching and learning process and pupil contact process.

It is vital that we are all aware of the necessary safeguards and protocols which must be adhered to and would therefore ask parents/guardians and pupils to read carefully the following information:

- It is expected that pupils and teachers engaging in Zoom/google meet video calls/recordings observe acceptable standards of appropriate behaviour and etiquette, as they would in a classroom setting, along with appropriate dress code during video calls
- St Patrick's Boys' National School code of behaviour and discipline rules remain in place.
- St Patrick's Boys' National School Child Protection Policy continues to remain in place during this period. Should a child protection concern arise during on-line classes or contact, staff members will follow the normal practice, in relation to dealing with such concerns.
- Video calling will be facilitated via invitations through email/class blog/google classroom.
- Zoom and google meet are the only platform that may be used for video calling.
- As learners access these services through their own devices, it is the responsibility of parents/guardians to review the data and privacy settings for their child's use of Zoom/google meets on the relevant devices.
- One-to-one video calls/contact may take place with the learner only with the prior consent of the parent/guardian. A consent form via Aladdin will be provided and must be completed.
- It is strictly prohibited for any pupil, parent/guardian or staff member to record and/or share in any manner, a live video call, either through a recording facility that may be available on the platform, or by using any other device e.g. mobile phone, without the express written consent of all parties involved in the call being obtained in advance and also acquiring the advance approval of the principal teacher. All parties should note that to record a call without consent is a serious issue which will be subject to disciplinary action under the relevant code of behaviour/disciplinary policy.
- As a matter of good practice, video calls which are conducted on a one-to-one basis with a student should only take place during normal school hours, and, it is required that a parent/guardian (or a responsible designated adult) be present during such calls, however, it will not be possible for the school to enforce this and take no responsibility for doing so. This should be arranged with the staff member in advance. It is recommended that a quiet place be provided for the call so it can proceed without undue interruption, but one which is in an area of the

home that is open and accessible to a parent/guardian (i.e. not in a bedroom behind a closed door).

- Where a staff member provides a video or audio recording of themselves by link to a recording hosted on the class blog, Parent(s)/guardians and pupils should be mindful that any such recording contains the personal data of the staff member. It is therefore prohibited for such recordings to be altered, downloaded to personal devices or shared with any other parties without the prior express written permission of the staff member.
- Where a learner is requested to submit a video or audio recording of him/herself for assessment, feedback etc., the staff member will specify how this is to be submitted using email, Class Dojo, google classroom.
- Recordings submitted as part of ongoing assignments/homework in the course of normal teaching and learning practice may be shared with teachers, school management and on school blogs within St Patrick's Boys' National School for teaching and learning purposes but will not be shared with any other parties. Learners should retain a copy of recordings submitted on their own devices in case of any query arising subsequent to the deletion of the recording, in the same way as written work is retained by the learner once it is graded and returned
- Where a phone call is required, staff may only access data available on Aladdin for their own pupils. Staff will block their number when making phone calls to parents.

Advice for Parents, Guardians and pupils:

- Ensure that the device you or your child uses for video calling has the necessary updates, such as operating system updates and software/antivirus updates.
- Ensure your security software and settings are up to date
- If, for technical or other reasons you cannot access or use the approved platform(s), please contact the relevant staff member to explore an alternative. However please note that it may not be possible to use alternatives suggested by parents/guardians if they do not meet data privacy and security requirements of St Patrick's Boys' National School.
- Please ensure you read over the services' privacy or data protection policy to be sure you are satisfied with how Zoom/Google meet manages your data, and to review the permissions you are granting.
- Ensure your device is being used in a safe and appropriate location and be sure to log out, mute and turn off video as appropriate.

Any queries in relation to data protection issues can be addressed to info@stpatricksboysns.com

Consent:

I have read the schools Internet Safety: Acceptable Use Policy and agree to abide by its contents:

Name of pupil:

Parents' Signatures:

Date:

Appendix 3 Appendix 7 – Online Safety

Technology, Internet and Social Media: Safe Use for Children and Young People

The Merriam-Webster dictionary defines Social Media as a *'form of electronic communication...through which users create online communities to share information, ideas, personal messages, and other content'*. Any website that enables users to interact is considered a social media site, including social networking sites (SNS) such as *Facebook*, *Instagram*, Snapchat and *Twitter*; gaming sites and virtual worlds such as *Club Penguin*, *Moshi Monsters* and the *Sims*; video sharing sites such as *YouTube*; and blogging sites such as *Tumblr*.

There are a number of possible motivations for Social Media usage, including:

- To connect with others with common interests and hobbies;
- To connect with friends, and make new ones;
- To browse the internet for information;
- To 'chat' with others, download music and play games;
- A need to belong and a need for self-presentation;
- To satisfy individuals' need for self-worth and self-integrity; Risks and Dangers

The sections below outline some of the risks and dangers associated with social media usage.

Access to inappropriate content, including pornography:

Children and young people may be exposed to illegal or unsuitable content online, such as:

- Pornography
- Child abuse images
- Dangerous advice encouraging eating disorders, self-harm or suicide
- Excessive violence or race hate materials
- Some websites show illegal content. Others that are legal might have unregulated advice or are meant for adults only.

Children may come across this content by mistake, or they may look for it because they are curious. Promises of special offers or prizes can also draw young people to inappropriate sites or material. Furthermore, many online games are free but offer the chance to buy items such as extra lives or new levels; children may run up big bills without realising it or provide personal details in order to receive 'extra lives' or game credits.

Harmful online communities:

Young people may also access websites which promote eating disorders such as anorexia, bulimia or self-harm. Harmful online communities can change the way young people see real life – even if they do not want that to happen.

Ignoring age restrictions:

Some websites and games use age restrictions and checks to make sure that children do not see unsuitable content. Children must be at least 13 year of age to register on most social

networking websites. However, verifying the age of a member is an issue.

'Friending' or communicating with people they don't know: Children and young people may 'chat' or become 'friends' with people on social networks or online games, even if they do not know them or have never met them in person. These people are unknown strangers and their public persona on social media does not necessarily reflect the reality of who they are or what their motives may be

Grooming and sexual abuse:
'Groomers' can use social media sites, instant messaging apps (including teen dating apps), or online gaming platforms to connect with a young person or child. They can spend time learning about a young person's interests from their online profiles and use this knowledge to help them build a relationship with the child or young person. It is easy for groomers to hide their identity online. For example, they may pretend to be a child and then chat and become 'friends' with children they are targeting.

Child sexual abuse on line:
When sexual exploitation happens online, young people may be persuaded, or forced, to send or post sexually explicit images of themselves, take part in sexual activities via a webcam or Smartphone, or have sexual conversations by text or instant messaging.
Abusers may threaten to send images, videos or copies of conversations to the young person's friends and family unless they take part in further sexual activity or pay the abuser money

Sharing personal information:
Privacy controls can limit who can see a child's details, like their name, age and where they live. However, when a child connects to someone as a 'friend', that person will have access to the child's personal information. Some 'free' games might ask a child to provide personal details before they can play; some will then illegally rent or sell this data on to others. Many apps and social networking sites use software to locate where the user is. Children and young people can also reveal their location by tagging photos on sites such as on Instagram or 'checking in' on Facebook or Foursquare. This means that people can find out where the child lives, socialises, works or studies.

'Sexting':
'Sexting' involves sending sexually explicit images, videos or text messages via ICT. Primarily such 'sexts' are sent using mobile phones and/or chat apps such as Snapchat, Viber and WhatsApp. The 'sext' can constitute child pornography.

Length of time online:
An ISPCC Survey on Children and the Internet (2011) found most children and young people (around half) said they spent 1-3 hours online per day. 9% of the secondary school aged group said they spent between 3-5 hours online per day. Less than 5% of the older young people said they didn't use the internet.

Just under half of the secondary school aged group said they accessed the internet at home in their bedroom (44%), rather than in a communal area at home; fewer children in the primary school aged group said they accessed the internet in their bedroom (23%).

The young people who spent longer online were found to be more likely to access the internet in their own rooms and to engage in more social activities online. Furthermore, young people

who spent longer online are also generally more likely to be exposed to all the elements and risks of the internet, including being more likely to give out personal details, not to use privacy settings, to meet up with someone from online and to access sites for the 18+ age group.

Connections between social media use and negative outcomes Researchers[8] have identified a number of negative outcomes which can be associated with excessive social media usage

Depression: A link has been identified between the amount of time spent on Facebook by high school students and their likelihood to experience depression.

Anxiety & Compulsive Behaviour: There are several studies linking social media to anxiety and compulsive behaviour. Younger generations (particularly the iGeneration[9] and Net Generation[10]) are checking in very often (defined as every hour, every 15 minutes, or all the time) with their messages and social networks. A new medical term has been created out of this constant connectivity. Phantom vibration syndrome, defined as perceived vibration from a mobile phone that is not vibrating, has been reported to occur with large numbers of people. Phantom vibration syndrome may reflect a manifestation of the anxiety that mobile phones elicit in those obsessed with checking in on their social media and messages.

Loneliness and Narcissism: Narcissistic personality disorder is marked by a grandiose sense of self-importance, fantasies of unlimited power, self-promotion, vanity and superficial relationships. Many studies show that social networking sites exacerbate narcissism. More time spent on Facebook and a higher frequency of checking Facebook predicted higher narcissism scores. Social media affects mental health by influencing how people view, maintain, and interact with their social network. Social media is so seductive because it allows for the illusion of companionship without the demands of friendship.

Diminished privacy: Another way that social media is changing how young adults interact with their networks of relationships is by changing the privacy of these relationships. The relationships people have on Facebook are visible to many, often resulting in a loss of privacy within personal relationships. Monitoring of others' activities on social media can lead to negative relationship outcomes such as online and offline relational intrusion, stress from 'defriending' and blocking, or students catching their 'significant other' cheating online. Bullying can also occur.

Fear of missing out & Diminished self-esteem: Fear of missing out refers to the blend of anxiety, inadequacy and irritation that can flare up while skimming social media such as Facebook, Snapchat, Twitter and Instagram. The worry that the fear of missing out signals in the mind is set off by the fear of 'regret'.

Social media users are often exposed to details about their peers' lives that were not actively sought out. Exposure to other people's activities can lead to users comparing their own social lives with that of their peers which subsequently may have harmful effects. Fear of missing out keeps people from being able to relax and be content with their particular circumstances because they are bombarded with the interesting activities of their friends. Fear of missing out can also foster a feeling of victimization and exclusion in young adults.

Making social comparisons was associated with lower self-esteem and more negative health outcomes. Use of the internet and social media has been linked to increased social

comparison and diminished self-esteem and self-image.
Research findings have shown that Facebook usage can be damaging to romantic relationships due to increased jealousy, partner surveillance and compulsive Internet use.

[9] Those born after 1994 who have grown up with smartphones and direct access to online content.
[10] Those born between 1982 and 1991 who have grown up with computers and the internet

The Impact of Sedentary Behaviours on Mental Health:
Sedentary behaviours, like those which social media usage encourages, have been linked to physical health risks, including: increased risk of type II diabetes, obesity, cardiovascular disease, high blood pressure and metabolic syndrome.

Several studies provide evidence that people with high levels of sedentary behaviour (for example, TV watching and computer use) have an increased risk of developing a depressive and/or anxiety disorder. While there is a connection between sedentary behaviours and mental health risks, it is unclear which one follows the other. People who spend more time in sedentary behaviours have less time for face–to-face social interaction and physical activity, both of which have been proven to be protective against mental disorders.

Social Media and ICT correlation with disrupted sleep patterns:

There is a correlation between disrupted sleep patterns and use of ICT and social media. One of the reasons for this is the effect of the particular lighting used to illuminate many screen devices which interferes with the brain's ability to produce the chemicals that help a person sleep. Browsing social media before bed is not just distracting from sleep; it can quite literally stop a person from being sleepy at all. This is particularly concerning as the connection between sleep and mental health is well documented.
Poor sleep can make people less receptive to positive emotions and a link has been identified between disrupted sleep patterns and depression.

Rapid task switching (also known as multitasking) encouraged by social media and ICT usage may also be a root cause of depression. While multitasking is inherently a human trait, technology has perhaps overly encouraged and promoted it. The current use of multi-window computer environments, multi-app Smartphone screens and the wide ranging sensory stimulation (and distraction) offered by high definition, customisable visual and auditory signals, coupled with tactile stimulation through vibrations, all contribute to reducing the ability to focus and increase an individual's vulnerability to depression.

Responses & Solutions

It is recommended that young people have an awareness of how online activities make them feel. For example if they feel anxious or sad, or if those online activities might be getting in the way of other interests that improve their overall mental health and wellbeing.

Parents should also be aware of the threats to mental health that their children can face. By understanding how social media can affect the mental health of their children, parents can talk to their children about social media habits, balancing their time on social media and ICT, and help protect their children from experiencing mental health issues later in life.

How do we safeguard children from the dangers of excessive internet usage?

- Keep up to date with developments in internet technology:
- Know what sites children are accessing, what they do on these sites, why they access these sites, who they have contact with, how long they are on the internet, what are their worries are while using the internet and what supports are available for children.
- Become familiar with social media language; for example, **LMIRL** (let's meet in real life), **ASL** (age, sex, location), **NIFOC** (nude in front of computer). The UK Child Exploitation and Online Protection Centre (Ceop) has identified a helpful guide to social media language[11]. It is essential that parents learn to identify warning signs of excessive or inappropriate ICT and social medial usage to aid early detection and intervention.
- Keep communication channels open with children. It can be helpful to discuss risky and safe behaviour (privacy settings, not using profile photos, not using own names), help to set up social networks, equip children with coping skills and information on where to get help, discuss opinions on the benefits and limitations of the internet, and talk to children about their online reputation.
- Set controls using security and filter software, supervise the time and place they use the internet, limit the time of access and regularly check user history.
- Create a healthy culture – agree basic usage rules together e.g. time limits and places of use (adults need to model these rules); make going online a daily event which allows adults to monitor and observe reactions

[11] http://parentinfo.org./article/online-teen-speak-updated

Aappendix 4

Children First

An Roinn Leanaí agus Gnóthaí Óige
Department of Children and Youth Affairs

TUSLA
An Ghníomhaireacht um Leanaí agus an Teaghlach
Child and Family Agency

Addendum to *Children First: National Guidance for the Protection and Welfare of Children*

Online Safety

Action Plan for Online Safety

This addendum is intended to supplement *Children First: National Guidance for the Protection and Welfare of Children* [DCYA, 2017] which are the national guidelines to assist professionals, organisations and individuals to recognise and report child abuse and neglect. It has been issued by the Minister for Children and Youth Affairs under section 6 of the Children First Act 2015 following a commitment made in the Government's Action Plan for Online Safety 2018 – 2019, which states:

> *"We will amend the Children First guidance to include a specific reference to the need to consider online safety in the context of completing the child safeguarding statement."*

Obligations on organisations to safeguard children and young people

One of the main objectives of the Children First Act 2015 is to ensure that children and young people are kept safe from harm while using the services of relevant organisations. The Act does this by placing the following specific statutory obligations on organisations:

- To keep children safe from harm while they are using the service
- To carry out a risk assessment to identify whether a child or young person could be harmed while using the service

The types of organisations and services that have statutory responsibilities under the Children First Act 2015 are listed in full in Appendix 1 of the Children First Guidance.

- To develop a Child Safeguarding Statement that outlines the policies and procedures which are in place to manage the risks which have been identified

- To appoint a relevant person to be the first point of contact in respect of the organisation's Child Safeguarding Statement

This addendum does not alter or increase these obligations. It has been published to clarify that organisations providing relevant services to children should consider the specific issue of online safety when carrying out their risk assessment and preparing their Child Safeguarding Statement.

Keeping children and young people safe from harm online

The Government's Action Plan for Online Safety notes that *"it is now almost impossible to imagine a world without the internet or to imagine a future where the internet has less of a role in our lives than it does today."*

It is important that we acknowledge the central role of the internet in all of our lives and that we support children and young people to take advantage of all of the unprecedented opportunities to learn, discover, create and communicate that new technologies provide.

However, while they are often confident and competent users of new technologies, children and young people may be less aware of the inherent risks involved. Children First operates on the premise that it is the responsibility of everyone in society to keep children and young people safe from harm. This responsibility includes keeping children safe from harm online.

Children should be supported and encouraged to develop safe and responsible online behaviours. If a relevant service is allowing children access to the internet where they could become exposed to harm, including harm of assault or sexual abuse (as set out in Section 2 of the Act), there is an obligation on the service provider to ensure that the risk is identified and that the policies and procedures that are in place to manage the risk are set out in the Child Safeguarding Statement. Further detailed information on undertaking a risk assessment is set out in the Children First: National Guidance for the Protection and Welfare of Children [DCYA, 2017] and Guidance on Developing a Child Safeguarding Statement [Tusla, 2017].

You should always contact Tusla if you have reasonable grounds for concern that a child may have been, is being, or is at risk of being harmed.

Guidance on what constitutes a reasonable concern is set out in chapter 2 of the Children First: National Guidance.

Concerns can be reported to Tusla using its web portal.

If you think that a child is in immediate danger and you cannot contact Tusla should contact the Gardaí without delay.

Further resources:

Children First: National Guidance for the Protection and Welfare of Children [DCYA 2017]

Guidance on Developing a Child Safeguarding Statement [Tusla 2017]

Child Safeguarding: A Guide for Policy, Procedure and Practice [Tusla 2017]

Be Safe Online: Ireland's Official Online Safety Hub [Government of Ireland]

www.webwise.ie

www.hotline.ie

www.watchyourspace.ie

Department of Children and Youth Affairs
January 2019