Stratford College
Co-educational Secondary School

Acceptable Computer User Policy (AUP) for Students

6th June 2019

Scope of Policy: Whole School

Mission

The aim of this Acceptable Use Policy is to ensure that pupils will benefit from learning opportunities offered by the school's Internet resources in a safe and effective manner.

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 Therefore, if the school AUP is not adhered to this privilege will be withdrawn and appropriate sanctions – as outlined in the AUP – will be imposed.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 pupils

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

Policy Content

General

- Students should have respect for the property, equipment and facilities of the school.
- Students must not enter the Computer Room without the supervision of a teacher.
- Staff or students may request to share the IT lab with another teacher who is then responsible for all the students present.
- Internet sessions will always 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.
- The school will regularly monitor pupils' Internet usage.
- Students will be made aware of "Plagiarism & Copyright" infringement and are subject to punishment if breached. More information can be found on the Stratford Library webpage under the "Information Literacy" Tab.
- Students are reminded that mobile phones should be left in their lockers. As part of the "User Policy for Mobile Devices in Stratford College" teachers will advise students if/when they may bring digital devices into the classroom for educational purposes.
- Continuous Professional Development training regarding Internet safety can be provided as may be relevant.
- 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 cloud storage of files by students in school must only be to upload and download files for educational purposes.

- Students will treat others with respect at all times and will not undertake any actions that may bring the school into disrepute.

Internet

- Students will not intentionally visit Web sites that contain obscene, illegal, hateful or otherwise objectionable materials.
- Students will pupils report accidental accessing of inappropriate materials in accordance with school procedures.
- Students will use the Internet for educational purposes only.
- Students will not copy information into assignments and fail to acknowledge the source (plagiarism and copyright infringement).
- Students will never disclose or publicise personal information. If it is necessary for educational purposes disclosing personal information should be done under the direction and supervision of a teacher.
- Downloading materials or images not relevant to their studies, is in direct breach of the school's acceptable user policy.
- Students 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.

Email, Social Media and Apps

- Students will use approved class email accounts under supervision by or permission from a teacher.
- Students will not send or receive any material that is illegal, obscene and defamatory, or that is intended to annoy or intimidate another person.
- Students 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, social media sites, chat rooms, discussion forums, apps or the internet.
- Students will note that sending and receiving email attachments is subject to permission from their teacher.
- Internet, app and social media communications should be undertaken only if directed and supervised by a teacher.
- Students will only have access to social media sites, apps, chat rooms, discussion forums, messaging or other electronic communication fora that have been approved by the school.

- Social media sites, apps, 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.

School Website

- Pupils will be given the opportunity to publish projects, artwork or school work on the World Wide Web in accordance with clear policies and approval processes regarding the content that can be loaded to the school's website
- The website will be regularly checked to ensure that there is no content that compromises the safety of pupils or staff.
- The publication of student work will be co-ordinated by a teacher.
- Pupils' work will appear in an educational context on Web pages with a copyright notice prohibiting the copying of such work without express written permission.
- The school will endeavour to use digital photographs, audio or video clips focusing on group activities. Content focusing on individual students will not be published on the school website without the parental permission. Video clips may be password protected.
- Personal pupil information including home address and contact details will be omitted from school web pages.
- The school website will avoid publishing the first and last name of individuals in a photograph, where they can be identified.
- The school will ensure that the image files are appropriately named – will not use pupils' names in image file names or ALT tags if published on the web.
- Pupils will continue to own the copyright on any work published.

Personal Devices

After considerable consultation with staff, parents and the Board of Management in the Spring of 2019, Stratford College has decided that

- **Phones, devices smaller than an iPad mini and tablets with 3G, 4G or any future 'G' capabilities are not allowed into the classroom,** nor can they be used during break-times, in the Library or supervised study. This list may change due to technological changes.
- Phones must be kept 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*).
- 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.

- **Mobile Phones,**
  a. **Mobile phones, devices smaller than an iPad mini and tablets with 3G, 4G or any future 'G' capabilities are not allowed into the classroom,** nor can they be used during break-times, in the Library or supervised study. This list may change due to technological changes.(as per our Acceptable User Policy).
  b. Phones must be kept 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

  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.
  Second Offence: If will be left in the office for three days and a parent must collect it.
  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.

Pupils 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.

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 Act 2018
- Child Trafficking and Pornography Act 1998
- Interception Act 1993
- Video Recordings Act 1989
- The Data Protection Act 1988
- Non Fatal Offences against the Person Act 1997

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

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

ACCEPTABLE USER POLICY FOR DIGITAL DEVICES IN STRATFORD COLLEGE

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 sign this section under the guidance of their Class Tutor.

- 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.
- **Phones, devices smaller than an iPad mini and tablets with 3G, 4G or any future 'G' capabilities are not allowed into the classroom,** nor can they be used during break-times, in the Library or supervised study. This list may change due to technological changes.
- Phones must be kept 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).
- At the start of each academic year students will sign this 'User Policy for Digital Devices in Stratford College' form which is in their school journal in conjunction with their form teacher. This form will be reviewed on a yearly basis due to technological dues and will be updated as necessary in the school journal.
- Usage of digital devices depends on a culture of trust and respect for self and others.
- Digital devices must not be shared with other students.
- Each student must have a set of earphones. Sound on digital devices will only be permitted as deemed suitable by the teacher.
- Digital devices must be insured by the owner and are the responsibility of the student. As per of our Code of Behaviour and Discipline Policy, see Property, Point 4, Stratford College will not be responsible for loss, damage or breakages to the digital device.
- **Wifi Hotspots are not allowed, and nor is 3G, 4G or any other future 'G' access to the Internet**.
- **Misuse of the digital device and/or breaking of the rules above will result in the device being confiscated for a week**. Each infringement will be noted on a student's school record.

Other disciplinary measures may be applied at the discretion of Stratford College, see code of behaviour.

- Stratford College may introduce further rules and regulations, as it sees fit, to reflect technological changes and/or feedback from students, staff and parents based on IT surveys administered at the start of each calendar year.

NOTE: SANCTIONS

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

- **Recommended Digital Device Specification for Students (Bring Your Own Device - BYOD)**

After considerable consultation with staff, parents and the Board of Management in the Spring of 2019, Stratford College is in a position to recommend the following specification when buying a student digital device needed for Teaching and Learning. The digital device should have the following functionality and peripherals:

- Windows 10
- Touchscreen
- Protective Case
- Stylus
- USB port(s)
- Keyboard
- Lightweight

At present the Microsoft Surface Go, or a digital device similar to it, is a digital device that supports our current specification requirements. The Microsoft Surface Go is available in two specifications, both of which are acceptable for school use:

- 64GB/Intel 4415Y/4GB RAM/Wifi
- 128GB/Intel 4415Y/8GB RAM/Wifi

Note: The term 'digital device' does not mean a smartphone or a device with 4G (or 5G) functionality. 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.

[Last updated: 30 May 2019]

Student Signature: _____ Date: _____

Parent/Guardian Signature: _____ Date: _____

Form Teacher Signature: _____ 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

Timeframe

June 2019 to June 2021

Approved

Date: 6th June 2019

Mr Cormac Murphy

Chair BOM

Ms Patricia Gordon

Secretary BOM

Appendix 1

ADVICE FOR APPROPRIATE ONLINE BEHAVIOUR

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.

Advice for Social Networking Sites:

On social networking sites, cyber bullying and harassment appear to be among the most prevalent problems and include the posting of nasty, mean or threatening messages on user profiles, as well as the setting up of fake profiles to poke fun at someone. The big difference between writing a nasty message on the back of your journal and posting it on the internet is that the messages can be seen by a very wide audience almost instantly.

Students should be aware of the consequences of engaging in cyber bullying as outlined in our Code of Behaviour and Discipline:

3. Online privacy, Cyber Bullying and code of behaviour

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. As part of such disciplinary action the Board of Management reserves t**he right to suspend or expel** a student or students where it considers the actions to warrant such sanctions.'

The Dos

- ☺ Do think carefully about how you present yourself when choosing a profile image. Your online reputation is important. Think also about he 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 offiline. 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