Acceptable Computer User Policy (AUP) for Students

18TH May 2015

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

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 Therefore, if the school AUP is not adhered to this privilege will be withdrawn and appropriate sanctions – as outlined in the AUP – will be imposed.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

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 mobile 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 memory sticks, CD-ROMs, DVDs or other digital storage media in school requires a teacher's permission.

- 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.

World Wide Web

- 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 use 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, if made available, 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

Pupils using their own technology in school, such as leaving a mobile phone turned on or using it in class, sending nuisance text messages, or the unauthorized taking of images with a mobile phone camera, still or moving is in direct breach of the school's acceptable use policy, unless under the supervision of a teacher for educational purposes, in which case the student must adhere to the "User Policy for Mobile Devices in Stratford College".

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 (Amendment) Act 2003

- Child Trafficking and Pornography Act 1998

- Interception Act 1993

- Video Recordings Act 1989

- The Data Protection Act 1988

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.

User Policy for Mobile Devices in Stratford College

This section will be included in the Student Journal. It may be updated annually in the Student Journal to reflect technological changes. At the start of every academic year each student must sign this section under the guidance of their Class Tutor.

1. Mobile device usage in the classroom is teacher-led. Teachers will tell the students when to bring in their mobile devices. They may not be needed for all classes or for every day.

2. 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.

3. At the start of each academic year students will sign a 'User Policy for Mobile 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.

4. Usage of mobile devices depends on a culture of trust and respect for self and others.

5. The mobile device remains in a student's locker and is turned off until it is required as decided by the teacher.

6. Mobile devices must not be shared with other students.

7. Each student must have a set of earphones. Sound on mobile devices will only be permitted as deemed suitable by the teacher.

8. Mobile 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 mobile device.

9. Wifi Hotspots are not allowed, and nor is 3G, 4G or any other future 'G' access to the Internet.

10. Misuse of the mobile 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 Sanctions of page 5 of this document.

11. 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.

Student 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

Timeframe

May 2015 to May 2017

Approved

Date: 18th May 2015

Mr Cormac Murphy   Ms Patricia Gordon

Chair BOM   Secretary BOM