STANTONBURY
International School

Online Safety Policy

Date: September 2020
Next review: September 2021

Background

This policy has been prepared by the school Online Safety Coordinator in association with the IT Systems Manager and the Designated safeguarding Lead. It consists of one main section on Online Safety with three annexes for:

- Further Information on Learning Platforms
- STAFF ICT Acceptable Use Policy
- STUDENT ICT Acceptable Use Policy

This Policy will be reviewed every year or more regularly as required and was last reviewed in October 2020 2020.

An audit will be carried out every two years by the Online Safety Coordinator, who will then review the policy. Any changes will be approved by the Head.

Introduction

The purpose of this policy is to protect the school and members of the school community from intended or unintended abuse via online activity.

This policy is intended to agree with the Online Safety – ICT Fair Use Policy for Staff written by the Griffin Schools Trust (GST).

The school recognises that online activity is increasing in society. It is useful as a communication tool and its content can be very beneficial and informative. We wish to prepare our students for a future that will involve safe use of online facilities. However, we all need to be aware of the potential legal implications and materials which could be considered abusive or defamatory.

Internet use is also an important element of teaching and learning and the school has a duty to provide students with quality internet access as part of their learning experience. Internet use is a statutory part of the school curriculum and a necessary tool for staff and students. The school internet access will be designed expressly for student use and will include filtering appropriate to the age of students. Students will be taught what internet use is acceptable, what is not and about the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation.

Students will be taught to be critically aware of the materials they read and be shown how to validate information before accepting its accuracy. Students use the internet widely outside of school and will need to learn how to evaluate internet information and to take care of their own safety and security.

The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer. The school cannot accept liability for the material accessed, or any consequences resulting from Internet use.

Scope

- The policy applies within school and at home when students and staff may use ICT equipment and/or access data being stored on school or third party computers.
- The Policy will be made available on the school website

- New staff will be asked to sign the Staff ICT Acceptable Use Policy to indicate that they have read it.
- All students will be asked to sign the Acceptable Use Policy, including students admitted in-year, to indicate that they have read it.
- The school wishes to acknowledge the use of Milton Keynes County Council Policies as a guide for the Staff Acceptable Use Policy.

Relevant legislation includes:

- Computer Misuse Act 1990
- Data Protection Act 1998
- Copyright, Designs and Patents Act 1988 Regulation of Investigatory Powers Act 2000
- Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
- We will also incorporate any changes that the new data protection act requires.

Purpose and Impact

- The Policy sets out to make users of ICT equipment and data safe by providing appropriate guidance.
- Breaches of this Policy and the Acceptable Use Policy by staff and students will be investigated and followed up as set out below.

Monitoring and Evaluation

- The IT technical support team may investigate breaches of the Acceptable Use Policy across the network and IT systems. Issues to investigate will be passed on to the Online Safety Coordinator.
- All staff and students will be expected to report any breaches of acceptable use and/or any Online Safety concerns to the Online Safety Coordinator.
- Each week the Online Safety Coordinator will review any breaches of the smoothwall filtering system and pass on issues that arise to tutors, HoY or safeguarding leads where appropriate.
- During lessons staff using ICT with a class will monitor student use.
- The Online Safety Coordinator will undertake an audit every year to ensure the policy is up to date.
- Methods to identify, assess and minimise risks will be reviewed yearly.

Roles and Responsibilities

The role of the Online Safety coordinator

- To keep a record of online safety breaches by students and deal appropriately with each one, informing the Designated Safeguarding Lead where there is a safeguarding issue or Prevent issue (following the school's procedures for safeguarding concerns). Serious issues will be discussed with the Head and appropriate actions and sanctions will be followed.

- Less serious breaches will be dealt with as behaviour issues and logged on the school behaviour management system, liaising with Year Leaders, Student Support Leaders and parents accordingly; any legal matters will be referred to the HR manager.

- The Head will be informed immediately of any breaches of this policy that may constitute criminal offence or a very serious safeguarding threat that affects a large number of students/ staff.

- Where staff have breached the Acceptable Use Policy, this will be referred initially to their senior line manager who will assess the level of infringement and take appropriate action. This could range from a counselling conversation to disciplinary action or dismissal if the breach is a criminal offence.

- To provide regular information for parents through the school's website. Parents and students will be made aware of the Online Safety area of the school website and the role of CEOP.

- To provide training for all staff every two years. All new staff will be asked to complete the training if they miss the two yearly cycle. Further training will be given relating to needs that occur locally or nationally for example training related to making staff aware of the way social media can be manipulated to recruit vulnerable students into extremism and how staff may respond swiftly and appropriately.

- To ensure that a cohesive and responsive programme of study is included in Year assemblies, the school PSHE programme and Learning About Life Days.

Re: Cyberbullying

- If the school / Online Safety Coordinator becomes aware of cyberbullying they will take steps to identify the bully by, where appropriate, examining system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police, if necessary.

- Sanctions for those involved in cyberbullying will follow the guidance set down in the school's Behaviour Strategy and Anti-bullying policies and will take account of other relevant DfE guidance, for example:

    - Parent/carers will be informed.
    - The bully will be asked to remove any material deemed to be inappropriate or offensive.
    - A service provider may be contacted to remove content.
    - Internet access may be suspended at school for the user for a period of time.
    - The police will be contacted if a criminal offence is suspected.

The role of the IT Systems Manager

- To ensure the security of the school information systems and users' data will be reviewed regularly and virus protection will be updated regularly.
- To inform the Online Safety Co-ordinator of serious breaches of the school's firewall and any other concerns regarding online safety.
- Breaches will be assessed by the IT technical team to establish and address any technical threats or concerns.
- Files held on the school's network will be regularly checked for viruses and other forms of malware.
- Unapproved software will not be allowed in users' work areas or attached to email.
- The Network Manager will review system capacity regularly.

- Access levels will be reviewed to reflect the curriculum requirements and age of students.
- The school's broadband access will include filtering appropriate to the age and
- maturity of students.
- To regularly (twice a half term) search through search engines and social media to check for undesirable content regarding the school. Any unfavourable content found will be passed on to the Online Safety Coordinator and the Head

The role of the Teacher

- All staff are required to complete Online Safety training every two years. This will be supplemented, when required, by face- to-face training and staff briefings in order to respond to national and local need.
- To report any breaches of the students' Acceptable Use Policy.
- To respond to concerns that students in their care may have with, where necessary, the support of the Online Safety Coordinator.
- To ensure all devises that are left in classrooms are locked or logged off to prevent unauthorised misuse.
- Teachers are encouraged to explore the use of new technologies to enhance learning and decrease staff workload; however, they must ensure the secure storage of sensitive data and risk assess the potential for misuse.
- To ensure Personal data pertaining to any student or member of staff should not be sent over the Internet or taken off site unless it has been encrypted.

The role of the Head teacher

- To support the Online Safety Coordinator when dealing with issues that may be breaches of the Acceptable Use Policy or detrimental to the school's reputation.

The role of the Stantonbury Governing board

- To complete Online Safety training every two years. This will be supplemented, when required, by face-to-face training in order to respond to national and local need.

The role of the student

- To report to staff any breaches of the Acceptable Use Policy.

The role of parents

- Parents' attention will be drawn to the school's Online Safety Policy through parent communications, other school publications and the school website.
- A partnership approach with parents will be encouraged.

The role of all staff

- If any member of staff becomes aware of any unacceptable online behaviour they must report it to the Online Safety Coordinator and / or the Designated Safeguarding Lead. This includes any aspects that relate to the Prevent Strategy.
- To inform the IT helpdesk if an unsuitable site is discovered being accessed in school: the URL should be reported to the IT Helpdesk.
- Any future ICT developments will be evaluated for risk and policies and practices amended to enable the new development to be embedded safely into school practice. This will need to be done with discussion between the member of staff suggesting changes, the Online Safety Coordinator, the IT Systems Manager and others as appropriate.

All staff are required:

- As part of their induction programme to read and sign the Acceptable Use Policy.
- To ensure where possible that the copying and subsequent use of Internet derived materials complies with copyright law.

Re: Email

- Email sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.
- The forwarding of chain messages is not permitted.
- Staff should not include e-mail content that is offensive, abusive or defamatory or unduly negative and should share information on a need-to-know basis; the copying of sensitive emails to large numbers of people is not acceptable practice.
- The same applies to emails conveying confidential and sensitive information about a student e.g. to communicate a child protection concern. These emails must contain the word SAFE in the subject line and should be deleted once they have been acknowledged by the Designated Safeguarding lead.
- Staff should not use personal email accounts to communicate with students or parents, or for any work-related business.
- Staff should not use personal email accounts during school hours.

Re: School website

- The website will include a Safeguarding section for students and parents where up-to- date information and links relating to Online Safety will be made available to students and parents. CEOP access is also available directly from this page.
- Staff or students' personal information must not be published.
- The website should comply with the school's guidelines for publications including respect
- for intellectual property rights and copyright.
- In keeping with the school's policy on the use of photographs, student's full names will not be used on the website with photographs.

Re: Social networking

- Staff must not add students as friends on social networking sites outside the school domain.
- Staff will consider their own professional reputation and that of the school when posting on any social networking sites.

Re: Use of school ICT and lap-tops:

- Staff should not make use of school ICT equipment, including laptops, for any business that is not related to their professional role at school. This includes storing personal photographs, internet shopping, browsing websites.

Protecting Personal Data

Personal data will be recorded, processed, transferred and made available according to the GDPR Regulations 2018.

Handling e-Safety Complaints

- Any complaint about staff misuse must be referred to the Head.
- Complaints of internet misuse will be dealt with by a member of SLT & the Safeguarding Team.

- Complaints of a safeguarding nature must be dealt with in accordance with school safeguarding procedures.

Annexes

1. Further information on Learning Platforms

Learning Platforms (LPs) include Sharepoint; SIMs, SISRA; Google Apps; and Virtual Learning Environments (VLEs)

- Only current students, parent/carers and staff will have access to the LP.
- Temporary access may be granted in appropriate situations to students from feeder primaries.
- A visitor may be invited onto the LP by a member of the SLT. In this instance there may be an agreed focus or a limited time slot.
- When staff, students etc leave the school their account or rights to specific school areas will be disabled.
- All users will be mindful of copyright issues and will only upload appropriate content onto the LP.
- Any concerns with content may be recorded and dealt with in the following ways:
  - The user will be asked to remove any material deemed to be inappropriate or offensive.
  - The material will be removed by the site administrator if the user does not comply.
  - Access to the LP for the user may be suspended.
  - The user will need to discuss the issues with a member of SLT before reinstatement.
  - A student's parent/carer may be informed.

The Online Safety policy covers use of technologies as listed below but not exclusively. Websites, Apps, Email, instant messaging, chat rooms, social media eg Facebook, twitter, mobile smart phones with text, video and / or web function, tablets, gaming devices, online games, learning platforms, VLE's, Blogs, Wikis, podcasting, video sharing, downloading, on demand TV and video, movies and radio / smart TV.

2. Staff ICT Acceptable Use Policy

As a professional organisation with responsibility for children's safeguarding it is important that all staff accessing ICT resources take all possible and necessary measures to protect data and information systems from infection, unauthorised access, damage, loss, abuse and theft. All members of staff have a responsibility to use the school's computer system in a professional, lawful, and ethical manner. To ensure that members of staff are fully aware of their professional responsibilities when using Information Communication Technology and the school systems, they are asked to read and sign this Acceptable Use Policy.

This is not an exhaustive list and all members of staff are reminded that ICT use should be consistent with the school ethos, other appropriate policies and the Law.

I. I understand that Information Systems and ICT include networks, data and data storage, online and offline communication technologies and access devices. Examples include mobile phones, PDAs, digital cameras, email and social media sites.
II. School owned information systems must be used appropriately. I understand that the Computer Misuse Act 1990 makes the following criminal offences: to gain

unauthorised access to computer material; to gain unauthorised access to computer material with intent to commit or facilitate commission of further offences or to modify computer material without authorisation.

III. I understand that any hardware and software provided by my workplace for staff use can only be used by members of staff and only for educational use. To prevent unauthorised access to systems or personal data, I will not leave any information system unattended without first logging out or locking my login as appropriate.

IV. I will respect system security and I will not disclose any password or security information. I will use a 'strong' password (A strong password has numbers, letters and symbols, with 8 or more characters, does not contain a dictionary word and is only used on one system).

V. I will not attempt to install any purchased or downloaded software, including browser toolbars, or hardware without permission from the system manager.

VI. I will ensure that any personal data of pupils, staff or parents/carers is kept in accordance with the Data Protection Act 1988. This means that all personal data will be obtained and processed fairly and lawfully, only kept for specific purposes, held no longer than necessary and will be kept private and secure with appropriate security measures in place, whether used in the workplace, hosted online (only within countries or sites with suitable data protection controls) or accessed remotely. Any data which is being removed from the school site (such as via email or on memory sticks or CDs) will be encrypted by a method approved by the school. Any images or videos of pupils will only be used as stated in the school policy covering images and photographs and will always take into account parental consent.

VII. I will not keep professional documents which contain school-related sensitive or personal information (including images, files, videos etc.) on any personal devices (such as laptops, digital cameras, mobile phones, USB sticks), unless they are secured and encrypted and approved by the school. Where possible I will use the Schools secured network storage or Sharepoint sites to upload any work documents and files in a password protected environment. I will protect the devices in my care from unapproved access or theft.

VIII. I will not store any personal information on the school computer system that is unrelated to school activities, such as personal photographs, files or financial information.

IX. I will respect copyright and intellectual property rights.

X. I will report all incidents of concern regarding children's online-safety to the Designated Safeguarding Lead and/or the Online Safety Coordinator as soon as possible (and within the same school day). I will report any accidental access, receipt of inappropriate materials, filtering breaches or unsuitable websites to helpdesk@stantonbury.org.uk.

XI. I will not attempt to bypass any filtering and/or security systems put in place by the school. If I suspect a computer or system has been damaged or affected by a virus or other malware or if I have lost any school related documents or files, then I will report this to the ICT Support Provider/Team (helpdesk@stantonbury.org.uk) as soon as possible.

XII. My electronic communications with pupils, parents/carers and other professionals will take place via work approved communication channels only e.g. via a school provided email address or telephone number. Any pre- existing relationships which may compromise this will be discussed with the Senior Leadership team.

XIII. My use of ICT and information systems will always be compatible with my professional role, whether using school or personal systems. This includes the use of email, text, social media, social networking, gaming, web publications and any other devices or websites. My use of ICT will not interfere with my work duties and will be in accordance with the school AUP and the Law.

XIV. I will not create, transmit, display, publish or forward any material that is likely to harass, cause offence, inconvenience or needless anxiety to any other person, or

anything which could bring my professional role, the school, or the Trust into disrepute.

XV. I will promote e-Safety with the pupils in my care and will help them to develop a responsible attitude to safety online, system use and to the content they access or create.

XVI. When using ICT with students I will ensure they are accessing suitable material.

XVII. If I have any queries or questions regarding safe and professional practise online either in school or off site, then I will raise them with the Online Safety Coordinator or the Designated Safeguarding Lead

XVIII. I understand that my use of the information systems, Internet and email may be monitored and recorded to ensure policy compliance.

XIX. I will participate in online safety training as required.

The School may exercise its right to monitor the use of information systems, including Internet access and the interception of e-mails in order to monitor compliance with this Acceptable Use Policy and the School's Data Security Policy. Where it believes unauthorised and/or inappropriate use of the service's information system or unacceptable or inappropriate behaviour may be taking place, the School will invoke its disciplinary procedure. If the School suspects that the system may be being used for criminal purposes or for storing unlawful text, imagery or sound, the matter will be brought to the attention of the relevant law enforcement organisation.

3. Student ICT Acceptable Use Policy

I. I will only use the ICT systems in school - including the internet, e-mail, digital video, mobile technologies, etc - for school purposes.

II. I will not download or install software on school computers or other devices.

III. I will only log on to the school network/ Learning Platform with my own user name and password.

IV. I will not reveal my passwords to anyone and I will change my passwords regularly.

V. I will make sure that all communications with other students, teachers or others when using the ICT systems is responsible, sensible and within the Law.

VI. I will fully participate in any activity that involves improving my knowledge of online safety.

VII. I will be responsible for my behaviour when using the Internet. This includes resources I access and the language I use.

VIII. I will not deliberately browse, download, upload or forward material that could be considered offensive or illegal. If I accidentally come across any such material I will report it immediately to my teacher.

IX. I will not give out any personal information such as my name, phone number or address. I will not arrange to meet someone unless this is part of a school project and approved by my teacher.

X. I will not take images of other students and/or staff without their permission. Where permission is given, the images will only be taken, stored and used for school purposes in line with school policy and will not be distributed outside the school network.

XI. I will ensure that my online activity, both in school and outside school, will not cause distress to my school, the staff, students or others or reflect badly on the school.

XII. I will not record, share or post hurtful or malicious material on social media in or out of school.

XIII. I will support the school approach to online-Safety and not deliberately upload or add any images, video, sounds or text that could upset or offend any member of the school community or bring the school into disrepute.

XIV. I will not invite or accept staff as friends on social networking sites whilst I am still a student at Stantonbury International School.

XV. I will respect the privacy and ownership of others' work on-line at all times.

XVI. I will not attempt to bypass the internet filtering system or to gain access to
XVII. others' accounts.

XVIII. I understand that all my use of the Internet and other related technologies
XIX. will be monitored and logged and can be made available to my teachers, parents and the police.

XX. I understand that these rules are designed to keep me safe and that if they are not followed, school sanctions will be applied and my parent/carer may be contacted. I also understand that if my use of ICT constitutes bullying, threats, abuse or potentially illegal activity that affects students or staff at the school, the school may involve the police.

XXI. I will report any behaviour by other students or staff that breaks this acceptable use policy.