EF ACADEMY

International
Boarding Schools

EF ACADEMY - TORBAY

E-Safety

Keeping students safe online and in the use of electronic resources

EF ACADEMY

International
Boarding Schools

Document title:	E-Safety
Date Created:	September 2016
Author:	Designated Safeguarding Lead
Individuals Involved in Developing the Document:	Head; Learning Technologies Co-ordinator; SLT
Document Purpose:	To promote and govern E-Safety responsibilities amongst staff and students
Related Documents:	Acceptable Use Policy Anti-bullying Policy Risk Assessment Policy Student Behaviour Policy Safeguarding Policy Staff Handbook
Date of Next Review:	September 2021
Change Log (what changes have been made, by who and when):	DCH, KLC, AH September 2016 AH January 2017 – Reviewed, staff code of conduct added MB June 2017 – Reviewed, reordered, Prevent subsection added RTA/AHA December 2018 – Reviewed and reordered, new staff names, AUP added to appendix 1 RTA/AHA September 2020 - addition on "Online School" internet safety and COVID-19 restrictions

The following documentation is also related to this policy:

- Safeguarding Policy
- Anti-bullying Policy
- Staff Code of Conduct for Electronic Resources and E-Safety
- Staff Code of Conduct within Safeguarding Policy
- Student Behaviour Policy
- Acceptable use Policy
- Keeping Children Safe in Education 2020
- Prevent Duty 2015

EF ACADEMY

International
Boarding Schools

Scope of the Policy

The Head and Executive Committee (Governing Body) have a legal responsibility to safeguard children and staff and this includes online activity.

As such, this policy is an integral part of our Safeguarding provision. This policy applies to all members of the EF Academy School community (including staff, students, volunteers and visitors) who have access to and are users of school ICT systems, both in and out of the school. This E–Safety Policy and its implementation will be reviewed annually.

The School fully appreciates the fundamental relationship between E Safety and Student Safeguarding and its legal obligations to safeguard all its students (See "Safeguarding Policy"). The School also recognises that the Education and Inspections Act 2006 empowers Heads to regulate reasonably the behaviour of students when they are away from the school site. This is especially pertinent to incidents of cyberbullying, or other E-Safety incidents, which may occur away from the school premises, but are linked to membership of the school. The 2011 Education Act gave greater powers to Heads with regard to the searching of electronic devices and the deletion of data.

The School will deal with E-Safety incidents with regard to this policy and other relevant policies ("Behaviour and "Anti-bullying" policies) and seek to keep Parents, Guardians and overseas offices fully informed of any E-Safety incidents as appropriate.

This policy takes into account guidance from the DfE, including statutory guidance in Keeping Children Safe in Education (Sept 2020), the Prevent strategy and advice from ISI as well as other appropriate organisations. It is published on our school website; further copies are available to parents and students on request.

The Internet is a vital tool for modern education; it is an essential part of everyday life for academic work and social interaction both in and out of school. We therefore have a duty to provide students with quality Internet access as part of their learning experience. We also have a responsibility to ensure that, from a young age and as part of their broader education, students understand the inherent risks, and learn how to evaluate online information and how to take care of their own safety and security in the digital world.

The school recognises that due to COVID-19 the need for online education has significantly increased to the extent that a student's timetable may be taught exclusively over the internet via a range of platforms. At times whole school learning may need to switch to online learning as the global situation develops. For example, March 2020 - June 2020 mandatory school closure and September 2020 - full school 2 week quarantine prior to attending lessons on site. This policy aims to ensure specific students, cohorts or the entire school student body can migrate to Online School/Blended Learning safely and quickly.

Internet use at EF Academy Torbay is intended to enhance and enrich teaching and learning, to raise educational standards and promote student achievement, to develop initiative and independent learning by providing access to information and to alternative viewpoints, to foster imagination and stimulate intellectual curiosity, and to

support the professional work of staff and enhance the school's management functions. For boarders, and in particular international boarders, the Internet is, along with the mobile phone, also a crucial means of keeping in touch with home and family.

Policy Aims

- To enable students to take full advantage of the educational opportunities provided by e-communication
- To ensure that, as a school, we work to develop in students the appropriate behaviours and critical thinking skills necessary to enable them to remain both safe and within the law when using the Internet and related technologies, both in the beyond the classroom.
- To inform and educate students as to what constitutes appropriate and inappropriate Internet usage
- To safeguard students and to protect them from cyberbullying and abuse of any kind derived from e-sources
- To help students to understand the range of risks inherent in the digital world – including but not limited to the risk of identity theft, bullying, harassment, grooming, stalking and abuse - and to take responsibility for their own online safety
- To ensure that the copying and subsequent use of Internet-derived materials by staff and students complies with copyright law
- To clarify the roles and responsibilities of students and staff in these respects
- To help protect the interests and safety of the whole school community and to provide guidance on how, as a school, we will deal with any infringements.
- To ensure specific students, cohorts or the entire school student body can migrate to Online School/Blended Learning safely and quickly (COVID-19).

EF ACADEMY

International
Boarding Schools

Managing E-Safety

As the School recognizes that E-Safety is part of the broader context of Safeguarding, therefore responsibility for managing issues relating to E-Safety at EF Academy Torbay fall within the scope of the responsibilities staff who have designated roles in respect of safeguarding and the School's approach to the use of technology. Those are:

Role	In post 2020 / 2021
Designated Governor for Safeguarding	Anna Ireland
Head (DSL)	Rob Tasker
Heads of Boarding (DDSLs)	Kelly Hall & Tina Desmond
Learning Technologies Co-ordinator (also E-Safety Coordinator)	Adrian Harrington
School Technology and Process Manager	Rob Murphy

Commented [1]: Additional people required here as the much of the responsibility to meet the requirements of the policy and regulations are signed off etc to off site staff/teams eg global IT etc

Roles and Responsibilities

Board of Governors
The Executive Committee is responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. The Designated Governor for Safeguarding has oversight of E-Safety as an extension of the School's duty to safeguard its students.

Head Teacher, DSL
The Head Teacher has a duty of care for ensuring the safety (including E-Safety) of all members of the school community, though the day-to-day responsibility for E-Safety, is delegated to the Learning Technology Coordinator. The Head Teacher is trained in E-Safety issues and reviews this document in liaison with the E-Safety Coordinator to help ensure all parties are aware of the potential for serious child protection and/or safeguarding issues to arise from:

- sharing of personal data
- access to illegal or inappropriate materials
- inappropriate online contact with adults/strangers/Online School
- potential or actual incidents of grooming
- cyber-bullying
- the threat of political radicalization and the importance of the Prevent duty
- the threat of Child Criminal Exploitation (CCE)

E-Safety Coordinator
The school's Learning Technology Coordinator, with responsibility for E-Safety :

- Takes responsibility for E-Safety issues and has a leading role in establishing and reviewing the school E-Safety policies and documents, including ensuring staff sign the staff handbook
- Coordinates with EF Global IT relating to network security

Commented [2]: Could we add ensuring staff sign to say they have read…?

Commented [3]: Form should be part of the staff handbook???????? Therefore main points from policy are in the handbook

Commented [4]:

Commented [5]:

EF ACADEMY

International
Boarding Schools

- Provides advice for staff & Host Families
- Liaises with Designated Safeguarding Lead (DSL) who will liaise with external authorities and consultancies where necessary
- Liaises with Governor responsible for safeguarding and the DSL to review reports of E-Safety incidents
- Attends relevant meetings of the Executive Committee as necessary
- Reports regularly to the SLT on E-Safety issues
- Promotes regular E-Safety events within the school to inform students and maintain the profile of the issue among the students and staff body

EF Global IT support, assisted by the Learning Technologies Co-ordinator is responsible for ensuring:

- that the school's technical infrastructure is secure on a day to day basis
- that filtering is applied and updated on a regular basis
- that they are up to date with E-Safety technical information
- that the use of the network is regularly monitored in order that any misuse or attempted misuse can be identified
- that monitoring software or systems are implemented and updated

The post-holders of these key pastoral roles are especially well placed to be alert to any changes in student behavior which might indicate a safeguarding concern and to discuss topical matters with students as they arise. All staff are trained in the Prevent duty.

Pastoral Managers and Head/Deputy Head of Boarding

These are key pastoral roles, the post-holders being especially well placed to be alert to any changes in student behavior outside of the school day, The Head and Deputy Head of Boarding line-manage House Parents and The Head of Boarding is the primary point of contact for Host Families if used Both ensure open lines of communication and escalating any potential safeguarding concerns to the DSL. The Heads of Boarding are trained in the Prevent duty and are both Level 3 safeguarding trained and registered as the School DDSLs.

Whole Staff Responsibility

All school staff have a responsibility to demonstrate, promote and support safe behaviours in their classrooms and to follow school E-Safety guidance. The code of conduct for staff at EF Academy Torbay, which is a part of the Safeguarding policy, contains more detailed information on this. Staff are provided with safeguarding updates, including E-Safety , as often as is necessary but at least annually.

Commented [6]: Could we add advice for host families here?

Commented [7]: . We have to (under Prevent) do a risk assessment of the school profile which should then determine our monitoring. This is worth a look: https://www.saferinternet.org.uk/advice-centre/teachers-and-professionals/appropriate-filtering-and-monitoring/appropriate-monitoring

Also of interest, monitoring can be outsourced to RM: http://www.rm.com/what-we-do/onlinE-Safety -for-schools

Commented [8]: I have created a questionnaire based on the suggestions of the above website for Global IT to complete and evidence to help form an appendix to this policy

EF ACADEMY

International
Boarding Schools

With regard to E-Safety , it is important that staff are vigilant to the material that students access online, both in school and residences during evenings and weekends. The Acceptable Use policy (Appendix 1) makes it clear that the School will monitor student use of systems, devices and networks. A culture of healthy interest and, where necessary, friendly challenge is encouraged. Staff should not feel like they cannot ask students what they are looking at and, accordingly, students should feel comfortable to approach staff to discuss anything concerning that they have seen online or in the online habits of others. Staff should pass on any such concerns to the DSL as a matter of urgency or in his absence the School DDSLs. All staff are trained in the Prevent duty.

Staff are responsible for ensuring that:

- they have read the Staff Acceptable Use of ICT Policy and signed the associated Code of Conduct Agreement
- they report any suspected misuse or problems to the E-Safety Coordinator
- digital communications with all members of the school community (students, parents, colleagues) must always be conducted on a professional level and only carried out using official school systems
- they monitor the use of digital technologies (mobile devices, cameras etc) in lessons and other school activities and implement current policies with regard to these devices
- internet use in lessons is pre-planned and closely monitored to ensure students do not gain access to inappropriate material.
- record and report any safeguarding concerns or disclosures relating to online safety to the DSL or DDSLs in the DSL's absence.

Student Responsibility

The vigilance of teachers and parents, boarding staff and guardians has an important part to play in the safeguarding and protection of students both at school and at home. However, young people have wide ranging access to the Internet, so the most effective form of protection ultimately lies in the good sense of young people and in their exercising judgement guided by a well-informed understanding of what is available to them and of the risks to which they are potentially exposed. For this reason, we work on the basis that students must be encouraged to be responsible for their actions, conduct and behaviour when using the Internet, much as they are responsible during classes or at other times in the school day. This is achieved through a targeted PSHE programme delivered by tutors, via Google Classroom information boards and through whole school assemblies as often as necessary and in conjunction with a fair and transparent disciplinary system.

Use of technology should be safe, responsible and legal. Any misuse of the Internet, inside or outside of school, will be dealt with in line with the school's Behaviour and Sanctions Policy.

Commented [9]: Right policy?

Students are responsible for:

- using the school's ICT systems in accordance with the Student Acceptable Use of ICT Policy
- reporting any instance of abuse, misuse or access to inappropriate materials to a member of staff
- knowing and understanding policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking / use of images and on cyber-bullying.

- understanding the importance of adopting good E-Safety practice when using digital technologies in school, Online Classes and out of school and realising that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school.

Prevent Duty and E-Safety

The Counter-Terrorism and Security Act 2015, places a legal responsibility on schools to take every effort to protect members of their community from the threat of political radicalization. Given the particular setting as an international boarding school, close attention is paid to the risk of online radicalisation and staff are updated regularly to our obligations under the Prevent duty.

We approach this issue in four ways:

1. **Providing a safe online environment.** We use appropriate filtering and monitoring systems, including physical monitoring by staff, and educate students to be aware of risks and how to communicate any concerns that they have to staff.

2. **Assessment of student behaviours.** We ensure a dedicated and knowledgeable staff: pastoral monitoring by tutors, Pathway Managers and the Head of Boarding is shared at least weekly with the Deputy Head and, where appropriate, causes for concern are notified to all staff in a weekly pastoral briefing.

3. **Staff training and information.** Relevant training, such as the Channel online general risk module, is widely promoted. The DSL ensures that staff are made aware of the risks of radicalization and the School's mechanisms for fulfilling its duties under Prevent as part of at least annual safeguarding updates. The DSL will be responsible for updating their own training as to Prevent, including completing online Prevent modules.

4. **Promoting fundamental values such as fairness, democracy, tolerance and the rule of law**. Through our PSHE and Tutorial programme, whole school assemblies, the curriculum and all other daily interactions between pupils and staff fundamental values are actively promoted. As with other safeguarding risks, all staff should be alert to changes in children's behaviour which could indicate that they may be in need of help or protection. Staff should use their judgement in identifying children who might be at risk of radicalisation and act proportionately.

Staff believing that a student is in immediate danger of becoming radicalised or of acting upon radical information can make a referral by phoning the confidential Anti-Terrorist Hotline on 0800 789 321 or emailing prevent@devonandcornwall.pnn.police.uk.

Commented [10]: Check to make sure correct

EF ACADEMY

International
Boarding Schools

Parents
Are responsible for:

- playing an important role in ensuring that their children understand the need to use the internet and mobile devices in an appropriate way. This is reflected in the School's Terms and Conditions which all parents sign and can discuss with international admissions offices.

Teaching and Learning

Internet use is an integral part of the curriculum and is a necessary tool for learning. The school has a duty to provide students with good quality internet access as part of their learning experience and recognises a duty to teach students how to evaluate internet information and to take care of, and responsibility for, their own safety and security.

The purpose of internet use in schools is to raise educational standards, to promote student achievement, develop research skills, to support the professional work of staff and to enhance the school's management functions.

Internet access is an entitlement only for those who show a responsible and mature approach to its use; the school reserves the right to withdraw it if it has concerns about the uses to which it is being put by any individual. Students will be taught what internet use is acceptable and what is not, and will be given clear objectives for internet use.

The school will strive to ensure that copying and the subsequent use of internet-derived materials by staff and students complies with copyright law. Students will be educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation; they will be taught to acknowledge the source of information used and to respect copyright when using internet material in their own work.

The above is more applicable than ever especially with the move to and use of Online School due to COVID-19 and the heightened number of hours students are expected to work online. Often 'Online' work will include independent study, remote from their teacher or peers, meaning students could be more vulnerable to online dangers than previously. It is acknowledged by the School that statistically, students with SEND may be more vulnerable to cyberbullying and abuse online than their peers.

Managing Information Systems

The security of the school information systems and users is managed by the organization's Global IT Department and will be reviewed regularly by the Learning Technologies Co-ordinator and Global IT.

EF ACADEMY

International
Boarding Schools

This includes

- Virus protection will be updated regularly
- Unapproved software will not be allowed in work areas or attached to e-mail
- Files held on the school's network will be regularly checked
- There will be a regular review of the school's system capacity conducted by Global IT
- The use of user log-ins to access the school's network systems will be enforced

Broadband Filtering:

The school's broadband access will include appropriate filtering. Breaches of filtering will be reported to the Learning Technologies Co-ordinator who will report the breach to Global IT and DSL. Offenders may be banned for a fixed period from the network, or, if the breach is such as to constitute a breach of the law, the incident will be reported to appropriate agencies such as the Police or CEOP.

If staff or students discover unsuitable sites, the URL will be reported to the school's Learning Technologies Co-ordinator who will escalate the concern as appropriate to Global IT who will take appropriate measures to block the URL.

Commented [11]: Update when new residence online

Monitoring and Usage:

Users should be aware that the school can track and record the sites visited and any searches made on the Internet by individual users. We would advise parents that we provide filtered access to the Internet for students but they should also be aware that, with emerging and constantly changing technologies, there is no absolute guarantee that a student will not be able to access material that would be considered unsuitable. The chance of just coming across such content is highly unlikely, but it obviously increases in direct proportion to the amount of time and effort an individual puts into their search. Anyone inadvertently coming into contact with such material must contact a member of staff immediately.

When using the Internet, all users are expected to comply with all laws and government regulations concerning copyright, libel, fraud, data protection, discrimination and obscenity. All staff are expected to communicate with students in a professional manner consistent with the guidelines set out in the Code of Conduct for staff at EF Academy Torbay (included in Staff Handbook). Access to the Internet in school is given to students on the understanding that they will use it in a considerate and responsible manner. Staff should ensure that students know and understand that, in addition to the points found in the section on 'Online activities which are not permitted' below, no Intranet or Internet user is permitted to:

- Retrieve, send, copy or display offensive messages or pictures
- Use obscene, racist or otherwise discriminatory language
- Harass, insult or attack others
- Damage computers, computer systems or computer networks
- Violate copyright laws
- Use another user's password or account

- Trespass in another user's folders, work or files
- Use the network for commercial purposes
- Download and install software or install hardware onto a school computer, whether legitimately licensed or not
- Intentionally waste limited resources, including printer ink and paper
- Use the school computer system or the Internet for private purposes unless The Head or other senior member of staff has given express permission for that use.

Careful consideration is also given to the use of 3G and 4G connection on site and the use of hotspots. The School aims to educate students in the safe use of the internet and social media and continually offers guidance and support. If the School suspects that a student is accessing inappropriate material through their own 3G or 4G network, then all devices are temporarily confiscated and searches carried out in line with the School's Rewards, Behaviour and Sanctions Policy.

Emerging Technologies:

Emerging technologies will be examined for educational benefit before use in school is allowed. Students will be instructed about safe and appropriate use of personal devices both on and off site in accordance with the school's Acceptable Use Policy.

Any evidence that mobile data is being used inappropriately will result in the device being confiscated and parents notified of the offence. It might be that students face disciplinary action in line with the E-Safety policy depending on the content accessed.

Personal Data:

Personal data will be recorded, processed, transferred and made available in accordance with the Data Protection Act 1998 and to GDPR 2018 (Data Protection Act 2018).

Bullying/Cyberbullying:

Cyberbullying, as with all other forms of bullying, of any member of the school community will not be tolerated. The school's anti-bullying policy applies in these cases. All incidents of alleged cyberbullying reported to the school will be recorded. Students, staff and parents/carers will be advised to keep records of the bullying as evidence. The school will take steps to identify the bully, where possible and where appropriate. This may include examining school system logs, identifying and interviewing possible witnesses, contacting the service provider (via Global IT) and, if necessary and appropriate, the police.

EF ACADEMY

International
Boarding Schools

Students must not use their own or the school's devices and technology to bully others either inside or outside the confines of school buildings. Bullying incidents involving the use of technology will be dealt with under the school's anti-bullying policy. If a student thinks s/he or another student has been bullied in this way, they should talk to a member of staff about it as soon as possible.

Sanctions for those involved in cyberbullying include all those for bullying, as well as potentially:

- The bully may be asked to remove any published material deemed to be offensive or inappropriate
- Global IT will liaise with the service provider may be contacted to remove content if the bully refuses, or is unable to delete content
- Internet access within school may be suspended for the user for a period of time
- Parents/guardians will be informed
- The police will be contacted if a criminal offence is suspected

If there is a suggestion that a student is at risk of abuse from his or her involvement in any form of online activity, the matter will be dealt with under the school's Safeguarding Policy. If any student is worried about something that they have seen on the Internet or in a social media context, they must report it to a member of staff about it as soon as possible. It is acknowledged by the School that statistically, students with SEND may be more vulnerable to cyberbullying and abuse online than their peers.

Network Passwords:

It is important that we take all reasonable measures to secure and protect the whole school community from online threats. Global IT maintains rigorous controls on password security and requires frequent changes. Staff must follow Global IT requirements for password changes otherwise they cannot access their accounts.

Staff have individual logins to access the school network and My Academy (or Alpha) and Google Apps for Education. It is important that staff understand and respect the need for complete password security.

All staff should:

- Use a strong password, which will need to be changed at regular intervals when prompted by the system
- Not write their passwords down
- Strictly never share passwords with anyone else.

Whilst students access the Internet through a password protected wifi SSID this is the same username and password for all students, however, browsing activity is logged against the Mac address of the device that is connected and in the case of mis-use this could be used to determine which device had been used.

Commented [12]: Again, will need to consider in our risk assessment but for now a solid placeholder.

Authorisation of Internet Access:

EF ACADEMY

International
Boarding Schools

The school will maintain a current record of all staff and students who are granted access to the school's electronic communication systems. All visitors to the school site who require access to the school's network or internet access should be asked to read and sign an Acceptable Use policy.

Commented [13]: How will this be done?

The school will take all reasonable precautions to ensure that users access only appropriate material. However, owing to the nature of internet content, it is not possible to guarantee that access to unsuitable material will never occur. Methods to identify, assess and minimise risks will be reviewed regularly.

Managing Email:

Staff and students receive a password protected email account on arrival at the school and this should only be used for professional and educational purposes.

- Staff and students must never communicate using personal email accounts
- All emails must be appropriate in terms of content and tone
- Students must notify a member of staff immediately if they receive offensive email
- Students must not reveal personal details of themselves or others in email communication, or arrange to meet anyone not known to them without specific permission
- Social email use during the school day can interfere with learning and will be discouraged
- Email sent to external organisations should be written carefully and authorised before being sent, in the same way as a letter written on school headed paper
- Staff and students should use school email accounts to communicate with students, and such communications must always be professional in tone, content and motivation
- Misuse of the email system could lead to disciplinary action being taken against staff or students
- Detailed rules and guidance for staff and students on email usage can be found in the Staff/Student Acceptable Use of ICT policy.

Managing Social Media:

Parents and teachers need to be aware that the Internet has a host of online spaces and social networks which allow unmediated content to be published. Students should be encouraged to think about the ease of uploading personal information, the associated dangers and the difficulty of removing an inappropriate image or information once published.

All staff should be made aware of the potential risks of using social networking sites or personal publishing either professionally with students or personally. Examples include: blogs, wikis, social networking, forums, bulletin boards, multi-player online gaming, chatrooms, instant messaging and many others.

EF ACADEMY

International
Boarding Schools

- The school respects privacy and understands that staff and may use social media forums in their private lives. Staff must not accept current school students as "friends" on social media sites. Nor should they discuss the school or students of the school on any social media platform.
- Teachers wishing to use social media tools with students as part of the curriculum should risk-assess the sites before use and check sites' terms and conditions to ensure the site is age-appropriate and password protected. If in any doubt, they should consult the School's Learning Technologies Co-ordinator.
- Staff should not be setting up social media tools as a means of communication with student's personal social media accounts for use on a personal or professional basis.
- Students are advised never to give out personal details of any kind which may identify them and / or their location. Examples include real name, address, mobile or landline phone numbers, school attended, IM and email addresses, full names of friends/family, specific interests and clubs, etc.
- Students are advised not to place personal photos on any social network space. They should think about how public the information is and consider using private areas
- Students should be advised on security and encouraged to set passwords, deny access to unknown individuals and instructed in how to block unwanted communications. Students should be encouraged to invite known friends only and deny access to others by making profiles private.
- Students are advised not to publish specific and detailed private thoughts, especially those that may be considered threatening, hurtful or defamatory
- Posts that, in the reasonable opinion of the school, could be deemed offensive or defamatory to individuals or to the school will be regarded as a serious breach of discipline and will be dealt with in the context of the school's behaviour policy.

Commented [14]: Added 22.2.2017

Commented [15]: Added 22.2.2017

Commented [16]: I think we need to bulk this up so it is clear that staff are not allowed to set up their own work accounts e.g. the current Facebook situation.

Commented [17]: Added 22.2.2017

Commented [18]: This needs to be clearly communicated to all staff

EF ACADEMY

International
Boarding Schools

Mobile Phones and Other Electronic Devices:

Guidance for staff on mobile phones and electronic devices can be found in the "Staff Acceptable Use" in Appendix 1 and on GlobalNet/staff handbook.

- Staff must not give their mobile phone numbers to students or seek to contact students by SMS "text" messaging
- The School recognises that mobile phones and other electronic devices can present a number of problems when not used appropriately:
- Mobile phones with integrated cameras could lead to child protection, bullying and data protection issues with regard to inappropriate capture, use or distribution of images of students or staff
- Their use can render students or staff subject to cyberbullying
- Internet access on phones and personal devices can allow students to bypass school security settings and filtering
- They are valuable items which may be stolen or damaged
- They can undermine classroom discipline as they can be used on "silent" mode
- Student use of electronic devices is governed by "Acceptable Use Policy"
- The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the school community and any breaches will be dealt with as disciplinary matters in conjunction with relevant school policies

- Students are permitted to bring mobile phones onto school premises but they remain the responsibility of their owners at all times. The school cannot be held responsible for any theft, loss of, or damage to, such phones suffered on school premises.
- Students may not bring mobile phones into examinations under any circumstances
- Phones may not be used to bully, harass or insult any other person inside or outside the school either through voice calls, texts, emails, still photographs or videos. Cyberbullying of this nature will bring severe penalties in accordance with the school's behaviour policy
- Any misuse of the Internet through Internet-enabled phones, such as downloading inappropriate or offensive materials or posting inappropriate comments on social networking sites, will be dealt with in accordance with the school's behaviour policy
- Phones must not be used to take still photographs or videos of any person on school premises without their express permission. Even if such permission is obtained they must under no circumstances be used to ridicule, harass, bully or abuse another person in any way
- Any unacceptable use of mobile phones will be dealt with in accordance with the school's behaviour policy
- The school reserves the right to confiscate for a fixed period the phone of any person contravening these protocols and to forbid them from bringing a mobile phone into school for any length of time deemed appropriate by the school

Commented [19]: Completely agree but needs careful communication to staff.

EF ACADEMY

International
Boarding Schools

Managing Photography and Video Capture on School Premises:

- Use of photographic material to harass, intimidate, ridicule or bully other students or staff members will not be tolerated and will constitute a serious breach of discipline
- Phones must not be used to take still photographs or videos of any person on school premises without their express permission. Even if such permission is obtained they must under no circumstances be used to ridicule, harass, bully or abuse another person in any way
- Indecent images taken and sent by mobile phones and other forms of technology (sometimes known as 'Sexting') is strictly forbidden by the school and in some circumstances may be seen as an offence under the Protection of Children Act 1978 and the Criminal Justice Act 1988. Anyone found in possession of such images or sending them will be dealt with by school authorities. If a student thinks that they have been the subject of 'sexting', they should talk to a member of staff about it as soon as possible
- The uploading onto social networking or video sharing sites (such as Facebook or YouTube) of images which in the reasonable opinion of the school may be considered offensive is a serious breach of discipline and will be subject to disciplinary procedures whatever the source of the material. In this context it makes no difference whether the images were uploaded on a school computer or at a location outside of the school
- Students, if requested, must allow staff reasonable access to material stored on phones and must delete images if requested to do so in any situation where there is any suspicion such images contravene school regulations. (Please see also the policy on Conducting a Search)
- If it has reasonable grounds to believe that a phone, camera, laptop or other device contains images, text messages or other material that may constitute evidence of criminal activity, the school reserves the right to submit such devices to the police for examination. (Please see also the policy on Conducting a Search)
- Such misuse of equipment will be dealt with according to the school behaviour policy and may involve confiscation and / or removal of the privilege of bringing such devices into school premises on a temporary or permanent basis.
- Due to COVID-19 restrictions, students should not 'screen record' or share any electronic recordings at any time. This includes Online Lessons which have been produced to support academic learning and our online students.

Managing other Electronic Equipment:

Students are permitted to bring other electronic devices such as Laptops, Mobile Technologies , Tablet Computers onto school premises with permission but they remain the responsibility of their owners at all times.

- The school cannot be held responsible for any theft loss of, or damage to, such phones suffered whilst at school
- No electronic device should be misused in any way to bully, harass or intimidate another person whether through text or images. Any such abuse will be dealt with in accordance with the school's behaviour policy
- No electronic device should contain inappropriate material such as violent or explicit videos or photographs, pornography or any material that could be considered offensive and / or inappropriate in a school context

EF ACADEMY

International
Boarding Schools

- Anti-virus software – it is advised all personal laptops should have appropriate anti-virus software that is regularly updated
- Network access – students may not access the school network from their laptop or any other mobile device other than with the student wifi SSID, EF Students. No student may use another's laptop without permission from that student
- Licenced software, distributing files / MP3s and Warez – no computer programmes (executables), MP3s, pornography, copyrighted material or material encouraging radicalisation may be distributed over the network. This includes the sending of files via email, as well as setting up 'servers' on students laptops and using them as a means of sharing software. Also, students should not download copyrighted material or nonshareware programs and should not be using their laptops as a means to view films, images, or graphics which are deemed inappropriate
- Audio – because computer audio can be distracting, the volume setting on laptops must generally be turned off when used during school time
- Games – computer games should never be played in class, during study time, and/or any scheduled lesson or activities unless part of a specified homework that is detailed in the student planner or permission granted by a member of staff. We fully appreciate that Games are part of our society and we do accept that Games can be played during lunchtimes, breaks and outside of the timetabled day as long as the following conditions are adhered to:
    - Games should be age appropriate and not contain offensive material in the form of images, sounds or graphics. The security of the network is maintained and Gaming does not impact on bandwidth and a reduction in the internet service. Students will be asked to remove them if they are deemed inappropriate or relates to network slowdowns or outages.

- Privacy – the school reserves the right to examine the hard drive on a student's personal laptop if there is reasonable suspicion that a computer is being used for inappropriate or potentially harmful purposes
- School owned laptops / netbooks /iPads - these must only be used under the supervision of a member of staff and must only be used for educational purposes. The uploading of inappropriate material such as images, software and graphics is forbidden and this includes the doctoring of screen savers and backgrounds.
- Consequences – students found in breach of these rules may have their Internet privileges removed, the privilege of using their technology at school removed either permanently or temporarily, and, depending on the seriousness of the breach, they may also have other sanctions imposed in accordance with school's behaviour policy.
- Due to COVID-19 restrictions, students should not share any Electronic equipment at any time. This includes mobile phones, tablet, laptops or other mobile devices. All school IT equipment will be sanitised between use.

EF ACADEMY

International
Boarding Schools

Responses:

All e–safety complaints and incidents will be recorded in the relevant student logs in My Academy; reports of bullying will be recorded and actions taken will be recorded.

Breaches of regulations will be dealt with according to the school's disciplinary and child protection procedures.

Many young people and adults find using the Internet and mobile phones a positive and creative part of their everyday life. Unfortunately, technologies can also be used negatively. When children are the target of bullying via mobiles phones, gaming or the Internet, they can often feel very alone, particularly if the adults around them do not understand cyberbullying and its effects. A once safe and enjoyable environment or activity can become threatening, harmful and a source of anxiety, therefore:

It is essential that students, staff and parents and carers understand how cyberbullying is different from other forms of bullying, how it can affect people and how to respond and combat misuse. Promoting a culture of confident users will support innovation and safety.

Bullying in any form, including cyberbullying, is not tolerated at EF Academy Torbay. Any instances of cyberbullying will be taken very seriously and dealt with thoroughly and appropriately in accordance with the school's anti-bullying and behaviour and sanctions policies.

In such cases, the Head Teacher will apply any sanction that is deemed appropriate and proportionate to the breach including, in the most serious cases, asking a student to leave the school. Misuse may also lead to confiscation of equipment in accordance with the school's policy on behaviour and sanctions.

Response to Incidents of Concern:

All members of the school community will be informed about the procedures for reporting E-Safety concerns, such as breaches of filtering, cyberbullying, accessing illegal content. The DSL will be informed of any E-Safety incidents involving Safeguarding and/or Child Protection concerns, which will then be escalated appropriately. The School will manage E-Safety incidents in accordance with the school sanctions policies where appropriate. The School will inform parents and/or guardians of any incidents of concern as appropriate.

Where there is a cause for concern that illegal activity has taken place then the DSL will report the concern to the police. If the School is unsure how to proceed with any incidents of concern, then agency or police advice will be sought. Students and parents will be informed of the complaints procedure. Any complaint about staff misuse will be referred to the Learning Technologies Coordinator and DSL in the first instance.

EF ACADEMY

International
Boarding Schools

Appendix 1

Acceptable Use Policy

As an EF staff member, you will have access to the Internet and Outlook email. Please adhere to the following EF guidelines regarding Internet access, use of social media and E-Safety . Internet access is not free; in fact, it is quite costly. To allow for optimal speed and access we have purchased increased network capacity and a high speed Internet connection. The intent of these expenditures, and the official policy, is that Internet access should be used for business purposes. Personal use of email and the Internet should be limited and must not have a negative effect on your work performance.

Our workstations and servers are protected using AntiMalware solutions that actively block requests to a list of websites, defined by category, and maintained by our software provider. Our networks provide a further layer of protection, using a different software provider to block access to illegal and malicious content, again defined by category and maintained by our software provider. We maintain a third list of websites, specifically and manually defined by our technology and academic staff, and used to block access by our students to distracting content

- Surfing pornographic websites for any reason is strictly prohibited.
- Downloading any unapproved programmes or licensed/copyrighted content to your computer is strictly prohibited. This includes, but is not limited to: videos, music files, games, and books. In addition, watching live video or listening to live radio from the Internet can dramatically slow down the entire network and is thus strictly prohibited.
- Unless clearly work-related, you may not use your EF-provided email address to subscribe to any email lists or newsgroups. All email and content on EF's servers and devices is the property of EF.
- Always maintain a professional relationship with students, never use your personal account/s for communication.
- It is prohibited to download on to your EF computer any non-work related or unapproved programmes from the Internet. This includes, but is not limited to, movies, videos, mp3 music files, and games.
- Many viruses are spread through email and instant messaging. When the recipient clicks a link or downloads a file containing a virus, the virus is then forwarded to everyone in the recipient's entire address book. Some viruses are not easy to detect. When clicking a link or opening a file you have received, always make sure you know and trust the sender. Those wishing to spread viruses often pose as trusted entities such as Amazon.com or Google. If you do not know the sender or are not sure, speak with your manager or contact IT. If you receive an email that is clearly suspicious, forward it to spam@ef.com and delete it from your Inbox.
- Promote internet safety to our students. While most of our students will already be experienced users of social media, they are potentially more vulnerable to abuse or bullying in that they are temporarily living and studying in another culture.

EF ACADEMY

International
Boarding Schools

- As part of internet safety all staff should be aware of the government Prevent strategy. As a school we should protect students from being targeted by groups that promote extremism and terrorism.

- As an EF staff member who uses our communication facilities, you may be involved in processing personal data as part of your job. Data protection is about the privacy of individuals, and is governed by the Data Protection Act 1998 and to GDPR 2018 (Data Protection Act 2018). Whenever and wherever you are processing personal data for the school you must keep it secret, confidential and secure, and you must take particular care not to disclose it to any other person unless authorised to do so. Do not use any personal data except as authorised by EF for the purposes of your job.

- Management reserves the right to change or alter this policy at any time.

- Any unlawful use of the Internet is strictly prohibited. Abuse of EF's electronic resources is grounds for discipline, including dismissal.

- Any E-Safety concerns should be reported to the DSL immediately.

EF ACADEMY

International
Boarding Schools

Appendix 2

Web Filters

The Web Filter is an E-Policy which is applied on your firewall to manage Web content. The Web Filter monitors millions of URLs. This policy protects staff and students from accessing inappropriate websites. This policy is applied on all networks (Cable and WIFI)

Below are the categories and sub categories which are blocked as part of our policy. The policy has been approved and provided by the Internet security team/Global IT.

Security Risk

- Malicious Websites
- Phishing
- Spam URLs
- Dynamic DNS

Adult/Mature Content

- Other Adult Materials
- Gambling
- Nudity and Risque
- Pornography
- Weapons (Sales)
- Marijuana

Bandwidth Consuming

- Peer-to-peer File Sharing

Potentially Liable

- Drug Abuse
- Hacking
- Illegal or Unethical
- Discrimination
- Explicit Violence
- Extremist Groups
- Proxy Avoidance
- Plagiarism
- Child Abuse

Staff can report sites that have been blocked incorrectly or report sites that should be blocked via Nemo or the Learning Technologies Coordinator

EF ACADEMY

International
Boarding Schools

Students can report sites that have been blocked incorrectly or report sites that should be blocked via their teacher.