EF ACADEMY

International
Boarding Schools

OXFORD E-SAFETY POLICY

Origins:	EF Academy Oxford E-Safety Policy May'16
Developed by:	Robert Murphy (School Technology and Process Manager) Paul Ellis (previous Head of School) Mark Fletcher-Single (previously Deputy Head Pastoral) Joan Wilisoni (previous Pathway Manager)
Document Purpose:	To promote the appropriate use of IT and safeguard students against inappropriate use.
Related Documents:	Academic Policy: InCo (previously SEND) Anti-bullying Policy Code of Conduct for Staff Complaints Policy Independent Listener Procedures Missing Student Procedure Safeguarding Policy Searching & Confiscation Policy Positive Mental Health & Wellbeing Policy Recruitment Policy Whistleblowing Policy Behaviour Policy Prevent risk assessment Data Protection (EF's Retention Periods Policy) GDPR Staff Factsheet Student Handbook Working Together to Safeguard Children December 2023 (DfE) Keeping Children Safe in Education September 2023 (DfE) DfE's publications Filtering and monitoring standards guidance and Cyber security standards The prevent duty: for schools and childcare providers June 2015 (DfE) Counter-Terrorism and Border-Security Act 2019 Revised Prevent Duty Guidance for England and Wales (April 2021) Protecting children from radicalisation: the prevent duty - Guidance for schools and childcare providers on preventing children and young people from being drawn into terrorism (updated August 2015). Working Together to Safeguard Children July 2018 (DfE) Keeping Children Safe in Education September 2022 (DfE), including: - Sexual violence and sexual harassment between children in schools and colleges (September 2021) - UKCIS Sharing nudes and semi-nudes: advice for education settings working with children and young people December 2020 - Mental Health and Behaviour in Schools (advice for schools) November 2018 (noting also Promoting and supporting mental health and wellbeing in schools and colleges June 2021, and a range of resources available including from Public Health England) - Preventing and Tackling Bullying (advice for schools)
Review log:	Aug.'18 - R. Murphy: GPDR incorporated into policy May'19 - P. Ellis & M. Fletcher-Single: school's responsibility to inform the Police if necessary, made clear (e.g. viewing terrorist material online) and other related policies ref.'d Jun.'20 - Mark Fletcher-Single: additional information and details of relevant procedural changes to incorporate the development of our COVID-19 Policy (incl. E-Safety of remote working), updates to reflect staff changes and changes to KCSiE in Sept.'20, and ref.'d to Norton security advice Aug.'21 - Mark Fletcher-Single: - developed information and details of relevant procedural changes to incorporate the development of our Covid-19 Policy

	- reviewed following advice from Barbara Lewin's Safeguarding training (Nov.'20) - reviewed to reflect the recent Feb.'21 consultation period of Boarding Schools: National Minimum Standards - reviewed to ensure greater procedural synergy with DfE's Teaching online safety in school (Jun.'19) - reviewed because of the School's leadership restructure during academic yr. Aug.'21 to Jul.'22 - updates to reflect staff changes and changes to KCSiE in Sept.'21 Sept.'22 - Mark Fletcher-Single: - reviewed to reflect the School's continued leadership restructure during academic yr. Aug.'22 to Jul.'23 - reviewed to reflect the changes to National minimum standards for boarding schools (from 5th Sept.'22) - reviewed to reflect change of DSL roles and updates to staff changes and changes to KCSiE in Sept.'22 Sept.'23 - Mark Fletcher-Single: reviewed policy to reflect the School's continued leadership restructure beginning from Sept.'23, updates to KCSiE Sept '23, and to ensure closer synergy with DfE's publications Filtering and monitoring standards guidance and Cyber security standards May '24 - Rob Tasker: Updated date reference of WTtSC to Dec 2023; DSL name change to RT; PM name change to KK; Reference to Orah platform; Change of governance from Exec. Committee to Senior Leadership Team (SLT). August '25 – RTA - additional requirements from KCSiE 2025 Sept '26 – RTA - additional requirements from KCSiE 2026 and to reflect new SLT and Boarding structures
Date of Next Review:	August '27

Data Privacy: GDPR

The GDPR is Europe's framework for data protection laws: it replaced the EU legislation which UK law was based upon. (GDPR stands for General Data Protection Regulation and it came into force on 25th May 2018). The EU's GDPR website says the legislation is designed to "harmonise" data privacy laws across Europe (which, of course, the UK was still in during its implementation) as well as give greater protection and rights to individuals. Compared to the UK's previously existing data protection laws, new rights for people to access the information companies hold about them, obligations for better data management for businesses, and a new regime of fines were introduced. A full explanation of procedures and more detail on the types of information held, can be found in the GDPR Staff Fact Sheet on the Internal Pages of EF Academy on Globalnet.

This policy takes into account guidance from the DfE, ISI, ISBA and other appropriate organisations. It is published on our school website; further copies are available to parents and students on request. EF Academy Oxford takes an effective whole-school approach to online safety to empower the School: protecting and educating students and staff in their use of technology, and establishing mechanisms to identify, intervene in, and escalate any concerns where appropriate.

Scope of the Policy

The Principal and EF Academy Oxford's Senior Leadership Team 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 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 the Education and Inspections Act 2006 empowers Principals/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 school premises, but are linked to membership of the School. The 2011 Education Act gave greater powers to Principals/Heads regarding 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 and risk assessments (e.g. Behaviour, Anti-bullying and EF Academy Oxford's Prevent risk assessment) 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.'23), the Prevent strategy, DfE's publications Filtering and monitoring standards guidance and Cyber security standards, advice from ISI as well as other appropriate organisations.

Statement on Internet and Social Media Use

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, 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.

Internet use at EF Academy Oxford 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 resident students, 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, 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, controlling behaviour and abuse, and to take responsibility for their own online safety.
- To ensure 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.

Classes within Online Safety

EF Academy Oxford understands the breadth of issues classified within online safety is considerable, and ever evolving, but can be categorised into four areas of risk:

Content: being exposed to illegal, inappropriate, or harmful content, for e.g.: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, and extremism.
Contact: being subjected to harmful online interaction with other users, for e.g.: peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.
Conduct: online behaviour that increases the likelihood of, or causes, harm, for e.g.: making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and / or pornography, sharing other explicit images and online bullying.
Commerce: risks such as online gambling, inappropriate advertising, phishing and or financial scams. If any students or staff are at risk, EF will report it to the Anti-Phishing Working Group (https://apwg.org/).

Responsibility for E-Safety

In as much as E-Safety is part of the broader context of Safeguarding, issues relating to E-Safety at EF Academy Oxford, fall within the scope of the responsibilities of those members of staff who have designated roles in respect of safeguarding and child protection. They are:
Rob Tasker (Deputy Head of School, **D**esignated **S**afeguarding **L**ead **DSL**)
Dona Jones (Principal, DSL Deputy)
Kate Krivich (Pathway Manager, DSL Deputy)
Alyona Lake (Pathway Manager, DSL Deputy)
TBC (Head of Boarding, DSL Deputy)

Student Responsibility
Limitations in the provision of hardware (such as filters and firewalls) and the vigilance of teachers and parents have 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 students must 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. Use of technology should be safe, responsible and legal.

Any misuse of the internet, inside or outside of school, will be dealt with under the School's Behaviour Policy. Sanctions will also be applied to any student found to be responsible for any material on his or her own or another website, such as Facebook for instance, that would constitute a breach of school rules in any other context.

Staff Responsibility

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 Oxford, 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. Regarding E-Safety, it is important staff are vigilant to the material students access online, both in school and at evenings and weekends. The Acceptable Use policy (Appendix 1) makes it clear 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 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.

Staff are responsible for ensuring:

- they report any suspected misuse or problems to the Designated Safeguarding Lead
- digital communications with all members of the School community (students, parents, colleagues, etc.) 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

Where a safeguarding report includes online elements or the sharing of images, **staff are reminded not to view or forward any illegal images** of a student but note what has been reported. Further guidance can be found in the "Sharing nudes and semi-nudes: advice for education settings working with children and young people". Where there is a safeguarding concern, the School will ensure the student's wishes and feelings are taken into account wherever possible and will work with them (and their families where appropriate) when determining what action to take and what services to provide. The School manages this by ensuring the student (and their family where appropriate) is included in discussions regarding next steps and methods of support. They will be encouraged to give feedback at all stages, and will be supported by their trusted adult, as appropriate.

Bullying

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.

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.

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
- parents / guardians will be informed
- the Police will be contacted if a criminal offence is suspected

Abuse

If there is a suggestion 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 policy for safeguarding and protecting the welfare of children and young people. If any student is worried about something 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.

Responses

- All E-Safety complaints and incidents will be recorded in the relevant student logs in Alpha (Salesforce); reports of bullying will be recorded under both the victim and perpetrator's account.
- Breaches of regulations will be dealt with according to the School's disciplinary and child protection procedures.
- Bullying in any form, including cyberbullying, is not tolerated at EF Academy Oxford. 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 rules and sanctions' policies.
- In such cases, the Principal or Deputy Head of School 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 discipline.

Principles and Acceptable use of the internet at EF Academy Oxford

Password Security

Staff have individual logins to access the School network Alpha (SIS), Orah and ManageBac. It is important 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 connected, and in the case of mis-use could be used to determine which device had been used.

Monitoring and Usage

Users should be aware the School can track and record the sites visited and any searches made on the internet by individual users. We advise parents we provide filtered access to the internet for students, and they are regularly reviewed for effectiveness. However, they should also be aware, with emerging and constantly changing technologies, there is no absolute guarantee 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. The leadership team and relevant staff have an awareness and understanding of the provisions in place for monitoring and are trained to know how to escalate concerns when identified.

When using the internet, all users are expected to comply with all laws and government regulations concerning copyright, libel, fraud, data protection, counter-terrorism, 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 Oxford (included in our Safeguarding Policy). Access to the internet in school is given to students on the understanding they will use it in a considerate and responsible manner. Staff should ensure students know and understand, 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 Principal or other senior member of staff has given express permission for that use

Managing Email

Email is the *sine qua non* of modern life and an immensely valuable tool for educational communication. However, it can also be a channel for cyberbullying, abuse and defamation. Spam, phishing and virus attachments can also make email dangerous. As a consequence:

- 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
- emails 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 should always use school email accounts to communicate with students, and such communications must always be professional in tone, content and motivation

Managing Social Media and Networking Sites

Parents and teachers need to be aware 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.
- The School will control access to social media and social networking sites because of the potential for harm inherent in such sites, particularly when used by younger students.
- 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 telephone numbers, school attended, IM and email addresses, full names of friends / family, specific interests and clubs, etc.
- Students are advised not to place personal photographs on any social network space. They should think about how public the information is and consider using private areas.
- Staff official blogs or wikis should be password protected. Staff must not run social network spaces for student use on a personal basis.
- 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.

Managing Mobile Phones

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.
- Mobile phones may be used in lessons only for educational purposes and only with the permission of the teacher.
- Phones may not be used to bully, harass insult or control 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 Anti-bullying and Behaviour policies.

- 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 and the Police contacted if necessary.
- 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.

Managing Photography and Video Capture on School Premises

- Use of photographic material to harass, intimidate, ridicule, bully or control 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, abuse or control 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 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 (see Searching & Confiscation Policy).
- If it has reasonable grounds to believe 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 (see Searching & Confiscation Policy).
- Such misuse of equipment will be dealt with according to the School's 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.

Photography and Filming by EF Academy Oxford

EF Academy recognises the use of photographs on websites and in other publications can pose direct and indirect risks to children and young people, and with regards to this we have put in place the following policy and procedure to address the safeguarding of our students:

- risk of identifying whereabouts of child or young person to groomers: even though the student's personal identity (full name, address) is kept confidential, we recognise other details accompanying the photograph can make them identifiable and therefore vulnerable to individuals looking to 'groom' children for abuse

- risk that photo itself may be used inappropriately by others: photographs can easily be copied and adapted, perhaps to create images of child abuse, which can then find their way on to other websites
- minimising these risks: we establish the type of images that appropriately represent the organisation and the activity, and we think carefully about any images showing children and young people on our website and in our publications and blogs
- we never supply the full name(s) of the student or students along with the image/s of any publications made public. e.g. for marketing purposes
- we only use images of children and young people in suitable dress, recognising some activities our students are involved, such as swimming, gymnastics and athletics present a higher risk for potential misuse than others (i.e. our photographs of these types of activities focus on the activity rather than a particular child or young person and avoid showing the full face and / or body: for e.g., any photographs in the sea or a swimming pool would show them in the water or from the waist or shoulders up only)

Reporting and Responding to Concerns regarding Photography and Filming
Students and parents are informed if they have any concerns regarding inappropriate or intrusive photography, these should be reported to the teachers / other staff member organising and / or hosting / supervising the event. These reported concerns are dealt with via the same procedure our other child protection and safeguarding issues, ensuring the DSL is informed by the staff member.

Managing other Electronic Equipment
Students are permitted to bring other electronic devices such as laptops, PDAs, tablet computers and mp3 players onto school premises with permission but they remain the responsibility of their owners at all times. They must keep them with them at all times or in a locked locker and must ensure they are appropriately made secure via passwords.

- 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 Anti-bullying and Behaviour policies.
- 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.
- Anti-virus software: all 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, lunchtime sessions or in after school clubs unless part of a specified homework that is detailed in the student planner or Google Classroom. These should be age appropriate and not contain offensive material in the form of images, sounds or graphics. These will be checked by a member of staff. Students will be asked to remove them if they are deemed inappropriate.

- Privacy: the School reserves the right to examine the hard drive on a student's personal laptop if there is reasonable suspicion a computer is being used for inappropriate or dishonourable purposes.
- School owned laptops / netbooks: 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 laptop, netbook, PDA or tablet PC 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 the School's Behaviour Policy.

Responses to Cyber Bullying
Please see the definition of cyberbullying given above.

- 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 and young people 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.
- It is essential 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.
- The DfE and Childnet have produced resources that can be used to give practical advice and guidance on cyberbullying (e.g. http://www.digizen.org/cyberbullying).
- Cyberbullying (along with all forms of bullying) will not be tolerated at EF Academy, whether the bullying originates inside or outside school. Activities conducted outside of school premises and outside of school hours that in our opinion constitute cyberbullying will also be covered by this policy. Instances of cyberbullying will be dealt with according to the School's Anti-bullying Policy. All incidents of cyberbullying reported to the School will be recorded.
- The School will take reasonable steps to identify the person(s) responsible for any instances of cyberbullying such as examining system logs, identifying and interviewing possible witnesses and contacting the service provider and the Police if necessary.
- Sanctions may include informing parents / guardians, the withdrawal of privileges, e.g. the person(s) responsible being instructed to remove any material deemed to be inappropriate, temporary or permanent exclusion in the most serious cases, and the Police being contacted if a criminal offence is suspected.

Review
Technology, and risks and harms related to it, evolve, and change rapidly. EF Academy Oxford will carry out an annual review of our approach to online safety, supported by an annual risk assessment that considers and reflects the risks our students face.

Sources
ISI guidance e-safety guidance and model policy issued by the ISBA
Becta www.becta.org.uk/safeguarding
Bristol LA's NGfL Learning Project
CEOP (Child Exploitation and Online Protection Centre www.ceop.police.uk)
Counter-Terrorism and Border-Security Act 2019
Kent County Council Schools and Settings eSafety Policy template

E-Safety from Safeguarding policy
The School's E-Safety Policy clearly sets out the School's procedures for mobile technology which includes the management of access to 3G / 4G. For more detailed guidance please refer to the E-Safety Policy. All staff must be aware and have read our Guidance on Home Teaching and Learning doc., too (please see below).


Guidance on Home Teaching and Learni

Guidance on Home Teaching and Learning
Home Teaching & Learning (HTL) will be implemented when a teacher(s) or student(s) is required to teach or learn from home due to an authorised absence *justifiable* inability to return to school. When HTL is implemented, the following guidelines are put in place. The intended outcome is the curriculum is at the forefront of the work and, as far as possible, student progress should not be negatively impacted. It is essential all staff understand the safeguarding measures outlined within this doc., e.g. '...ALL Zoom lessons should be recorded and uploaded.', 'Teachers must be professionally dressed.', etc. and our Safe Professional Practice guidelines.

Cybercrime
Cybercrime is criminal activity committed using computers and / or the internet. It is broadly categorised as either 'cyber-enabled' (crimes that can happen off-line but are enabled at scale and at speed on-line) or 'cyber dependent' (crimes that can be committed only by using a computer). Cyber-dependent crimes include:

- unauthorised access to computers (illegal 'hacking'), for e.g. a school's computer network to look for test paper answers or change grades awarded
- denial of service attacks or 'booting' - these are attempts to make a computer, network or website unavailable by overwhelming it with internet traffic from multiple sources, and
- making, supplying or obtaining malware (malicious software) such as viruses, spyware, ransomware, botnets and Remote Access Trojans with the intent to commit further offence, including those above

Children and young people with particular skill and interest in computing and technology may inadvertently or deliberately stray into cyber-dependent crime. If there are concerns about a student in this area, the DSL (or a deputy), should consider referring into the Cyber Choices programme. This is a nationwide Police programme supported by the Home Office and led by the National Crime Agency, working with regional and local policing. It aims to intervene where young people are at risk of committing, or being drawn into, low level cyber-dependent offences and divert them to a more positive use of their skills and interests. Cyber Choices does not cover 'cyber-enabled' crime such as fraud, purchasing of line and child sexual abuse and exploitation, nor other areas of concern such as on-line bullying or general online safety.

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.
- 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.