Online Safety Policy

This policy is applicable to the Stephen Perse Foundation (the 'Foundation') including those pupils in the Early Years Foundation Stage (**EYFS**).

Contents

1. About this policy

At the Foundation we have a strong pedagogical philosophy of linking digital learning to our students' curriculum to help enhance and develop learning as well as ensuring we are helping to prepare our students for the current world that they are living in. We aim to support our students in becoming flexible, fluid learners who are happy and confident to adapt to future changes. We are aware that raising the profile of digital learning in our schools means that we must have a robust strategic plan which ensures that our students are able to experience all that is on offer within a safe, structured environment.

This policy sets out the Foundation's safety expectations of staff, parents and students, in respect to the use of the Internet, e-mail, messaging systems and related technologies provided by the Foundation, and to all Foundation users accessing these services within the Foundation and from home.

This policy is designed to express the Foundation's philosophy and vision with regard to the Internet and digital communication in general. It aims to set general principles users should apply when using the services at the Foundation, but this guidance cannot and does not attempt to cover every possible situation.

2. Review Procedure

There shall be ongoing opportunities for staff to discuss with the DSL and/or DDSLs any issue of e-safety that concerns them.

The policy shall be amended if new technologies are adopted or there are changes in the regulations or guidance in any way.

This policy has been read, amended and approved by Heads of Schools, the Principal and Governors.

It has been agreed by the Senior Leadership Teams (SLT) (3-11 and 11-18) and the Foundation Leadership Team (**FLT**) and the Governors, that the policy shall be reviewed every year and/or after any serious incident. Any incident will be recorded in our e-safety incident logs held centrally in each school.

3. Introduction to online safety

Digital Learning (**ICT**) is seen as an essential resource to support teaching and learning within school, as well as playing a role in the everyday lives of our students. The Foundation needs to build in the use of these technologies to prepare our young people with the skills to access lifelong learning and employment. It is also important to recognise the constant and fast paced evolution of ICT within our society as a whole. Currently the Internet technologies young people are using both inside and outside of the classroom include:

- Websites
- Virtual Learning Environments
- Email
- Instant Messaging
- Chat Rooms
- Social Networking
- Blogs and Wikis
- Podcasting
- Video Broadcasting
- Downloading Music
- Apps that have been designed for either mobiles, tablets or laptops
- Gaming devices with web functionality
- Mobile Phones / Tablets with text, video and/or web functionality
- Smart Watches

Whilst exciting and beneficial, both in and out of the context of education, much digital learning, particularly web-based resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these Internet technologies.

At the Foundation**,** we understand the responsibility to educate our staff, parents and students about online safety issues; informing all stakeholders about the most up to date guidance available through staff training, parent workshops and for students, through assemblies and the curriculum.

This policy and the Acceptable Use Policies (for all staff, governors, visitors and students) are inclusive of both fixed and mobile Internet technologies provided by the Foundation (such as PCs, laptops, tablets, webcams, digital video equipment, etc.) and any personal device of this nature that is used or can be used for work purpose.

Measures Taken

At the Foundation we have created a safe digital learning environment consisting of the following elements:

- **Web Filtering/Monitoring** - Web filtering is handled by our firewall, it detects the user or device that is logged in and applies the appropriate level of filtering. The different filters are 3-11, Senior School (Lower and Upper), 6th Form and Staff. The categories that are blocked in each filter are decided either by the Heads of School or a member of the relevant SLT or FLT. Please refer to the Appropriate Filtering and Appropriate Monitoring sections for more detail.
- **Safesearch** - Safesearch facilities have been enabled for the major search engines and streaming media sites where possible. SSL (Secure Sockets Layer) Inspection is also enforced for student traffic which allows secure content to be inspected to detect search terms.
- **Port and Service Restrictions** - Access has been given to only essential ports and services through the firewall.
- **App Control** - There are several ways in which applications are restricted. The firewall has an application filter that detects specific app traffic at web level. This has been locked down to prevent student access to Proxy/VPN and Peer to Peer traffic. Our antivirus software also has an application filter that prevents potentially malicious application traffic running from a PC or Mac. Our group policy settings prevent apps being run from a user profile which helps prevent malware and ransomware.
- **Mobile Device Management (MDM) -** All student issued devices are managed and controlled by the Foundation's IT Department. All school devices are restricted so only approved apps can be installed. These apps are approved by Digital and Curriculum Leaders.
- **Device Access Outside of School -** Senior School and Sixth Form students are allowed to take their school mobile tablet devices home. The MDM restrictions are applied to devices both in and out of school. Restrictions to web services (filtering, port blocking etc) are applied from Year 1 through to Year 11 and there is a separate single filter that applies to all. There may be cases where this is not always applied out of school. If that is the case a student may have unrestricted web access unless there are any controls set on the router/firewall they are connected to. If parents have any concerns about this they are encouraged to contact the Foundation for more information. For devices that are set to use the filtering systems outside of school, activity is logged but not always actively monitored outside of hours on school days. During periods of national, or localised lockdown it may be deemed necessary for groups of pupils in Years 1 - 6 to be granted access to a Foundation device to support access to their curriculum whilst working remotely from school. At this point pupils will be required to log in to the school's firewall which will enable filtering measures as outlined above (device access outside of school).

Appropriate Filtering

Web filtering at the Foundation is via transparent proxy on the firewall. Web filter categories are agreed by the heads of school. Requests for individual blocking or allowing of sites can be made by a member of staff and checked by a member of the IT team. If they are unsure on a particular site they will consult with a designated safeguarding person.

At the Foundation we follow guidelines from the UK Safer Internet Centre in order to comply with Keeping Children Safe in Education (KCSIE). They state:

Inappropriate Online Content
Recognising that no filter can guarantee to be 100% effective, schools should be satisfied that their filtering system manages the following content (and web search)

Discrimination: Promotes the unjust or prejudicial treatment of people on the grounds of the protected characteristics listed in the Equality Act 2010
Drugs / Substance abuse: displays or promotes the illegal use of drugs or substances
Extremism: promotes terrorism and terrorist ideologies, violence or intolerance
Malware / Hacking: promotes the compromising of systems including anonymous browsing and other filter bypass tools as well as sites hosting malicious content
Pornography: displays sexual acts or explicit images
Piracy and copyright theft: includes illegal provision of copyrighted material
Self Harm: promotes or displays deliberate self harm (including suicide and eating disorders)
Violence: Displays or promotes the use of physical force intended to hurt or kill

What we do:
Discrimination: We block the Discrimination category for all students.
Drugs / Substance abuse: We block the Drug Abuse category for all students.
Extremism: We block the Extremist Groups category for all students.
Malware / Hacking: We block the Proxy Avoidance and Hacking category.
Pornography: We block the Pornography category for all students.
Piracy and copyright theft: We block the Plagiarism category for all students.
Self Harm: There is no specific category for Self Harm in the firewall but all abuse categories are blocked for all students.
Violence: We block the Explicit Violence category for all students.

Appropriate Monitoring

We have monitoring strategies that are designed to be in compliance with the government guidance document KCSIE, taking advice from the UK Safer Internet Centre.

Physical Monitoring - Pupils in Kindergarten to Year 5 in the 3-11 environment are closely supervised and do not have access to devices without a member of staff present. Pupils in Year 6, with a 1:1,

iPad should not be using their iPad between lessons. All teachers are able to monitor Foundation managed mobile tablet devices in the classroom, this allows them to view screens and lock devices.

Internet and Email Monitoring - All Internet and school email activity that goes through the Foundation systems is logged. Reports of web activity (including search terms) for all students in Year 6, Senior School, Sixth Form and those accessing the Foundations web filters from home are sent at regular intervals to the Designated Safeguarding Lead (**DSL**) and the appropriate Deputy Designated Safeguarding Lead (**DDSL**). As 3-11 students (with the exception of Year 6) share devices, a device search terms report is also sent. The reports contain a vast amount of information and detail so it is not feasible for all activity to be checked. However, if there is a particular concern or issue raised about a student, their web activity (using the reports as reference) and email history will be analysed. Random spot checks of users in the reports may be done for safeguarding and pedagogical reasons.

Active Monitoring - In order to actively identify "at risk" students whilst at school, potentially preventing a safeguarding incident, email alerting has been set up. This means that if students search for a particular keyword, the DSL or appropriate DDSL will be alerted via email. They will then be able to assess whether further investigation is required. They will be able to use the web activity reports mentioned above as a reference to check for any further online behaviour that is cause for concern. The keywords list is subject to change and determined by the Safeguarding Team with guidance from various industry sources. In addition to the keywords, email alerts are sent to the DSL and appropriate DDSL when a student attempts to access a website in high risk categories. Due to the high volume of alerts and the fact they could come in outside of school and term times, it is not feasible to expect an immediate response to them.

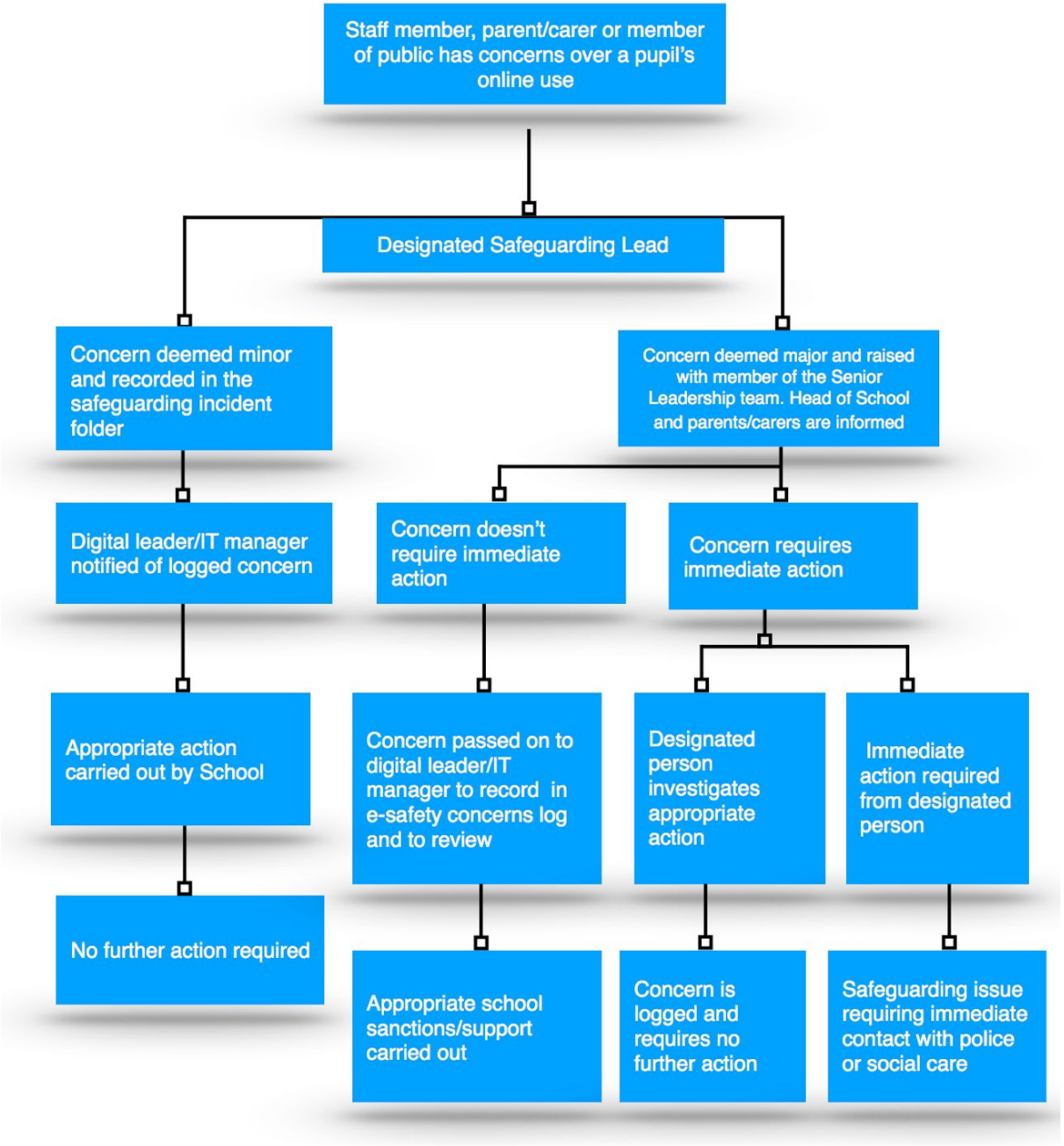
4. Roles and responsibilities

The Principal and Governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. The named designated persons within each school can be found in the Safeguarding and Child Protection Policy which is published on our website.

All members of the Foundation community have been made aware of who holds this post. Any online safety concerns will be logged through the Foundation's reporting systems and they will be actioned as necessary.

In regards to responsibilities for staff using technology remotely for teaching, please refer to the Remote Teaching Procedures for Staff document.

Flowchart showing action to be taken in the event of concerns over a students' online use



It is the role of the SLTs to ensure that all staff members at the Foundation are kept abreast of current issues relating to e-safety, with guidance through organisations such as Cambridgeshire LEA, Essex LEA, CEOP Command (Child Exploitation and Online Protection), ThinkUKnow and Childnet.

Senior Management and Governors are updated by the digital leaders and all Governors have an understanding of the issues and strategies at the Foundation in relation to local and national guidelines and advice.

This policy, supported by the Foundation's Acceptable Use Policies which can be found here:

- 3-11
- Senior School
- Sixth Form

protects the interests and safety of the whole Foundation community. It supports the following mandatory school policies: Safeguarding and Child Protection, Health and Safety, Behaviour and Discipline, Anti-Bullying as well as PSHEE in the curriculum and the home-school agreements.

The Foundation's Responsibility
As stated earlier, online safety covers a wider scope than just the Internet. The Foundation includes the following in the Online Safety Policy:

- The Foundation has appointed teachers who are digital leaders and oversee provision for online safety alongside the network manager and PSHEE coordinators, the DSL and DDSLs.

- The digital leaders, DSL and DDSLs can request and access support and advice from outside agencies such as the relevant local Children's Safeguarding Board and where necessary, the Police.

- The digital leaders, DSL and DDSLs will maintain the Online Safety Policy, manage online safety training and keep abreast of local and national e-safety awareness campaigns.

- The Foundation shall update the online safety policy as required and review the policy annually to ensure that it is current and considers any emerging technologies.

- The Foundation's IT Manager shall consult with Heads of School to audit the Foundation's filtering systems to ensure that inappropriate website categories are blocked.

- The Foundation will ensure that students and staff are adhering to the policy, by logging any incidents of possible misuse, and ensuring that these are investigated, where appropriate, by a member of the relevant Senior Leadership Team, the DSL or DDSL or the Police.

- The Foundation shall consider online safety whenever members of its community are using the Internet and ensure that every student has been educated about safe and responsible use.

- Students and staff need to know how to minimise online risks and how to report a problem, if in school or at home.

- All staff shall agree and sign the Acceptable Use Policy.

- Rosedale House, Dame Bradbury's and Senior School parents shall sign and return the relevant Acceptable Use Policy on behalf of their child. Sixth Form students shall sign and return the Acceptable Use Policy themselves.

Implementation

No policy can protect students without effective implementation. It is essential that staff remain vigilant in planning and supervising appropriate, educational ICT experiences. Online safety awareness is an essential element of all staff and volunteer induction. Training is therefore delivered to cover the following points:

- Students should be reminded of their responsibilities whenever they are using the Internet.
- Ensuring all staff, students and parents know how to report an incident of concern regarding Internet use.
- A member of the relevant SLT approves the Foundation's web filtering configuration.

Responsibilities and Expectations of Foundation Staff

Information technologies are developing rapidly and can leave staff unsure of best practice or how to discuss online safety issues with students. Advice and training for staff shall be incorporated into Child Protection Training which all staff must complete during their induction to the Foundation and every 3 years. All staff must be signed off to state that they have attended this training.

There will be additional online safety training provided through twilight training sessions run after school and on whole Foundation INSET days. New and relevant information, which needs to be brought to the attention of all staff immediately, will also be incorporated into safeguarding briefings (issued when new legislation, serious case reviews or in response to in-house issues), our own Foundation Daily News and in staff briefings.

All staff shall sign an Acceptable Use Policy for staff on appointment and re-sign a new policy if any significant amendments are made. Staff know and accept that the Foundation can monitor network and Internet use to help ensure staff and student safety.

The IT Department is responsible for the web filtering on all Foundation devices whilst onsite.

If a member of staff suspects a student of viewing or using inappropriate or illegal content, it must be reported to the DSL or DDSL. Staff must be aware of dangers to themselves in managing ICT use; for instance, if staff view inappropriate images to investigate their source, this needs to be reported to the DSL or DDSL immediately.

Any allegation of inappropriate behaviour by staff must be reported to the relevant SLT and investigated with care. Advice should be sought from the DSL and / or Cambridgeshire or Essex Police.

Email, text messaging, Social Networking and Instant Messaging (IM) all provide additional channels of communication between staff, parents and students. Inappropriate behaviour can occur and communications can be misinterpreted. When sending parents or students an email, staff must only use the Foundation's mailing systems. Staff must not give out their own personal email address. If a

member of staff receives an email that is offensive in any way they need to notify the e-Safety Officer or a senior member of staff so that the matter can be investigated further.

It is essential that staff do not accept students or parents as friends or "follow" them on social networking websites – until there is no longer any professional responsibility for the student (when the student has left the Foundation). Staff must ensure their personal social media accounts do not risk the reputation of themselves or the Foundation and suitable privacy settings are applied where necessary. Foundation social media accounts require approval from either the Marketing and Communications Manager or a member of the relevant SLT.

Internet chat rooms and online forums pose risks for staff and students. Whilst they can offer many positive experiences, there is widespread concern about their potential abuse by paedophiles attempting to groom new victims. The advice is that staff should not use unregulated chat rooms for children and should be aware that it is impossible to determine the age of any participant in these environments. They must not enter into any newsgroups, chat or interactive messaging discussion areas that are not primarily for education professionals without consulting a member of the relevant SLT.

Staff should be aware that students may be subject to cyberbullying via electronic methods of communication both in and out of school. If a student informs staff that this is happening staff have an obligation to report this to the e-Safety Officer or appropriate pastoral leader of the student. Staff must not investigate an issue themselves, or ask a student to investigate.

The Heads of School are aware that they have the power "to such an extent as is reasonable" to regulate the conduct of students off site (Education and Inspections Act 2006). Therefore, staff are able to confiscate items such as mobile phones etc. when they are being used to cause a disturbance in class or otherwise contravene the school behaviour/anti-bullying policy (Education and Inspections Act 2006). It must be noted that staff must not examine devices themselves but they should be handed to the e-Safety Officer, a member of the relevant SLT and potentially the police for investigation.

Protection of Foundation accounts and data is vital. Reference should be made to the Technology Acceptable Use policy for staff for further information.

Images that have been taken of students using either a Foundation camera or video camera shall be removed from the camera and stored on the computer system within the Foundation and not anywhere else. Staff need to take particular care with sharing features to make sure images are not synced to other unsecured or unauthorised devices. Location settings should be appropriately configured to keep the location of staff and students private.

5. Laws to be aware of that relate to e–safety Legal Framework

Many young people and indeed some staff use the Internet regularly without being aware that some of the activities they take part in are potentially illegal. The law is developing rapidly and changes occur frequently. Please note this section is designed to inform users of legal issues relevant to the use of communications, it is not professional advice.

Racial and Religious Hatred Act 2006
This Act makes it a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

Criminal Justice Act 2003
Section 146 of the Criminal Justice Act 2003 came into effect in April 2005, empowering courts to impose tougher sentences for offences motivated or aggravated by the victim's sexual orientation in England and Wales.

Sexual Offences Act 2003
It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). This can include images taken by and distributed by the child themselves (often referred to as “Sexting”). A person convicted of such an offence may face up to 10 years in prison.

The offence of grooming is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. (Typically, teachers, social workers, health professionals, counsellors etc. fall in this category of trust). Any sexual intercourse with a child under the age of 16 commits the offence of rape.

Communications Act 2003 (section 127)
Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

Data Protection Act 2018
The Act requires anyone who handles personal information to notify the Information Commissioner’s Office of the type of processing it administers, and must comply with data protection principles when treating personal data relating to any living individual. The Act also grants individuals rights of access to their personal data, compensation and prevention of processing.

The Computer Misuse Act 1990 (sections 1 - 3)
Regardless of an individual's motivation, the Act makes it a criminal offence to:

- gain access to computer files or software without permission (for example using someone else's password to access files);
- gain unauthorised access, as above, in order to commit a further criminal act (such as fraud); or
- impair the operation of a computer or program (for example caused by viruses or denial of service attacks).

UK citizens or residents may be extradited to another country if they are suspected of committing any of the above offences against or in another country.

Malicious Communications Act 1988 (section 1)
This legislation makes it a criminal offence to send an electronic message (email) that conveys indecent, grossly offensive, threatening material or information that is false; or is of an indecent or grossly offensive nature if the purpose was to cause a recipient to suffer distress or anxiety. This can include racist, xenophobic and homophobic comments, messages etc.

Copyright, Design and Patents Act 1988
Copyright is the right to prevent others from copying or using the author's "work" without permission. The material to which copyright may attach (known in the business as "work") must be the author's own creation and the result of some skill and judgement. It comes about when an individual expresses an idea in a tangible form. Works such as text, music, sound, film and programs all qualify for copyright protection. The author of the work is usually the copyright owner, but if it was created during the course of employment it belongs to the employer. It is an infringement of copyright to copy all or a substantial part of anyone's work without obtaining the author's permission. Usually a licence associated with the work will allow a user to copy or use it for limited purposes. It is advisable always to read the terms of a licence before you copy or use someone else's material. It is also illegal to adapt or use software without a licence or in ways prohibited by the terms of the software licence.

Public Order Act 1986 (sections 17 - 29)
This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006, it also makes the possession of inflammatory material with a view of releasing it a criminal offence.

Obscene Publications Act 1959 and 1964
Publishing an "obscene" article is a criminal offence. Publishing includes electronic transmission.

Protection from Harassment Act 1997
A person must not pursue a course of conduct, which amounts to harassment of another, and which he/she knows or ought to know amounts to harassment of the other. A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him/her is guilty of an offence if he/she knows or ought to know that his/her course of conduct will cause the other so to fear on each of those occasions. This also includes incidents of racism, xenophobia and homophobia.

Regulation of Investigatory Powers Act 2000

The Regulation of Investigatory Powers Act 2000 (**RIP**) regulates the interception of communications and makes it an offence to intercept or monitor communications without the consent of the parties involved in the communication. The RIP was enacted to comply with the Human Rights Act 1998. The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, however, permit a degree of monitoring and record keeping, for example, to ensure communications are relevant to school activity or to investigate or detect unauthorised use of the network. Nevertheless, any monitoring is subject to informed consent, which means steps must have been taken to ensure that everyone who may use the system is informed that communications may be monitored. Covert monitoring without informing users that surveillance is taking place risks breaching data protection and privacy legislation.

Criminal Justice and Immigration Act 2008

Section 63 makes it an offence to possess an "extreme pornographic image". This includes "explicit and realistic" images of an act which "threatens a person's life, … results or is likely to result in serious injury to a person's anus, breasts or genitals, … involves sexual interference with a human corpse" or a person performing a sexual act on "an animal (whether alive or dead)" (section 63(7)). Penalties can be up to 3 years imprisonment.

Education and Inspections Act 2006

The Education and Inspections Act 2006 outlines legal powers for schools which relate to cyberbullying/bullying.

Headteachers have the power "to such an extent as is reasonable" to regulate the conduct of students off site.

School staff are able to confiscate items such as mobile phones etc when they are being used to cause a disturbance in class or otherwise contravene the school behaviour/anti-bullying policies.

Keeping Children Safe in Education 2020

This is statutory guidance from the Department for Education (the **DfE**) issued under Section 175 of the Education Act 2002, the Education (Independent School Standards) Regulations 2014, and the Non-Maintained Special Schools (England) Regulations 2015. Schools and colleges in England must have regard to it when carrying out their duties to safeguard and promote the welfare of children.

Reviewed: November 2020

Version Control

Date of adoption of this policy	26 November 2020
Date of last review of this policy	17 November 2020
Date for next review of this policy	Autumn Term 2021
Policy owner	Director of IT
Authorised by	Vice Principal and Heads of Schools