HIGHGATE WOOD SCHOOL

Digital Safety Policy 2019

Ratified by the Governor’s Finance & Resources Committee: 16 September 2019	
This Policy is due for review September 2021 (Every 2 years)	

‘**Making a positive difference** to students’ achievements and experiences, maintaining the **highest expectations** and inspiring **self-belief**’

Everyone matters

Where the term “parent(s)” is used please read “parent(s) or person(s) with parental responsibility

Contents

Background / Rationale

The Internet and other digital technologies are powerful tools that provide many benefits to teaching and learning. They help teachers, students, parents, carers and the wider school community communicate with each other, share information and access educational content. They can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. Moreover, these technologies have become integral to the lives of children and young people in today's society, both within school and in their lives outside. However, despite the clear benefits, they also present risks.

These dangers include:

- Access to illegal, harmful or inappropriate text, images, video and other on-line content.
- Unauthorised access to/loss of/sharing of personal information
- The risk of "identity theft" or identity impersonation (eg catfishing)
- The impact of a negative digital footprint
- Inappropriate communication / contact with others, including strangers and the risk of being subject to grooming, indoctrination or radicalisation by on-line predators.
- Failure to properly evaluate the quality, accuracy and relevance of content found on-line or not adopting an appropriately critical view of information .
- Plagiarism and copyright infringement, including the illegal downloading of music, video and program files.
- Cyberbullying
- The risks presented by viruses, phishing and malware.
- The potential for excessive use which may impact on the social and emotional development and learning of the young person.

Whilst the use of filtering and monitoring systems makes it possible to guard against some of these risks, it is impossible to eliminate them completely. It is therefore essential, through good educational provision, to build digital literacy within our users, including the critical faculties to question, the personal resilience to cope with, and the confidence and skills to handle the existing and emerging dangers that digital technologies present.

This Digital Safety policy will demonstrate how Highgate Wood School provides the safeguards to manage and reduce risks, while also addressing wider educational issues in order to help young people (and their parents / carers) and their teachers to be responsible users and stay safe while using the internet and other technologies for educational, personal and recreational use.

Development / Monitoring / Review of this Policy

This Digital Safety policy has been developed by a working group made up of: the school's digital-safety lead, teachers, support staff, admin staff, governors, parents and carers, students

Consultation with the whole school community has taken place through the following: Staff meetings, School Council meetings, School Assemblies, Meetings of the Governing Body, Parent Information Evenings, and throughthe school website and newsletters.

Schedule for Development / Monitoring / Review

The implementation of this policy will be monitored by the **Digital Safety Lead**

Monitoring will take place **annually**

The Governing Body / Governors Sub Committee will receive a report on the implementation of the Digital Safety policy (which will include anonymous details of incidents) **annually**

The Digital Safety Policy will be reviewed annually, or more regularly in the light of any significant developments in the use of the technologies, new threats or incidents that have taken place. The next anticipated review date will be **Spring, 2021**

The school will monitor the impact of the policy using: Logs of reported incidents

Internal monitoring data for network activity: Surveys / questionnaires of students, parents\carers and staff

Scope of the Policy

This policy applies to all members of the school community (including staff, students, governors, volunteers, parents / carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of school.

The Education and Inspections Act 2006 empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of students when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other e-safety incidents covered by this policy, which may take place out of school, but are linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data.

The school will deal with such incidents within this and associated policies and will, where known, inform parents / carers of incidents of inappropriate online behaviour that take place out of school.

This Digital Safety policy takes consideration of the wider legislative framework, including GDPR and Data Protection legislation, Freedom of Information Act, the communications and Malicious Communications Acts, and the Computer Misuse Act, See Appendix A for a comprehensive list of relevant legislation.

Roles and Responsibilities

The following section outlines the roles and responsibilities for e-safety of individuals and groups within the school:

Governors:

Governors are responsible for the approval of the Digital Safety Policy and for reviewing its effectiveness. This will be carried out by the Governors / Governors Sub Committee receiving regular information about digital safety incidents and monitoring reports. A member of the Governing Body has taken on the role of Digital Safety Governor

- The role of the Digital Safety Governor will include:
- regular meetings with the Digital Safety Lead
- regular monitoring of digital safety incident logs
- reporting to relevant Governors' committee.

Headteacher and Senior Leadership Team:

The Headteacher is responsible for:

- ensuring the safety (including e-safety\digital safety) of members of the school community, though the day to day responsibility for e-safety\digital safety will be delegated to the Digital Safety Lead.
- ensuring that the Digital Safety Lead and other relevant staff receive suitable CPD to enable them to carry out their roles and to train other colleagues, as relevant
- ensuring the Senior Leadership Teaml receive regular monitoring reports from the Digital Safety Lead.
- being aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff. [1]

Digital Safety Lead:

The Digital Safety Lead will

- lead the Digital Safety working group
- take day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety/digital safety policies / documents
- ensure that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- provide training and advice for staff
- liaise with the Local Authority and other external organisations when required
- receive reports of digital safety incidents and create a log of incidents to inform future plans regarding online and digital safety
- meet regularly with Digital Safety Governor to discuss current issues, review incident logs and filtering / change control logs
- attend relevant meeting / committee of Governors
- reports regularly to the rest of the Senior Leadership Team

Teaching and Support Staff

Teaching and support staff are responsible for ensuring that:

- they have an up to date awareness of e-safety\digital safety matters and of the current school digital safety policy and practices
- have appropriate safeguards when accessing, saving, moving and using data that may be considered sensitive or personal.

[1] See Appendix A for flowchart

- they have read, understood and signed the school Staff Acceptable Use Agreement (AUA)[2]
- they report any suspected misuse or problem to the Digital Safety Lead for investigation / action / sanction
- they report any suspected online safeguarding concerns, including sexting, to the Designated Safeguarding Lead for investigation / action / sanction
- digital communications with students should be on a professional level and only carried out using official school systems
- e-safety\digital safety issues are embedded in all aspects of the curriculum and other school activities[3]
- students understand and follow the school Digital Safety Policy and Student Acceptable Use Agreement
- students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations

Designated Safeguarding Lead

The designated safeguarding lead will ensure all safeguarding officers are aware of the potential for serious child protection issues arising from:

- sharing and posting of personal data
- access to illegal / inappropriate materials
- inappropriate on-line contact with adults / strangers
- potential or actual incidents of grooming
- cyber-bullying

It is important to emphasise that safeguarding issues that happen online or through technological means must still be handled as safeguarding issues and the DSL always informed as a priority.

Students

Students are required to agree to the Student Acceptable Use before being given access to school systems and

- are responsible for using the school ICT systems in accordance with the Student Acceptable Use Agreement
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- are expected to know and understand the school policies on behaviour, including the use of mobile phones, data protection and the use of photographs.
- students should know and understand school protocols on the taking / use of images, on bullying and on cyber-bullying.
- should understand the importance of adopting good digital safety practice when using digital technologies out of school and realise that the school's Digital Safety Policy and Acceptable Use Agreement their actions out of school, if related to their membership of the school

[2] See Appendix for AUAs

[3] See Department Digital Guidance folders include ukfcis "Education for a Connected World" and other documents to support digital literacy within the curriculum. See G:\Digital Literacy

- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- make appropriate use of online resources, including Show My Homework, e-praise and Sam Learning

Parents / Carers

Parents / Carers play a crucial role in ensuring their children adopt safe and appropriate digital behaviours and are asked to

- support their child's online conduct in line the Student Acceptable Use Agreement.
- take advantage, where appropriate, of the opportunities provided by the school to support Digital Safety and Digital Literacy
- make use of the online tools available for parental contact, including Parentmail, Show My Homework and e-praise.

Community\Guest Users

Community and Guest users who access the school ICT systems will be expected to sign a Guest User AUA before being provided with access to school systems.

Policy Statements

Education – students

The education of students in digital safety is an essential part of the school's safety provision. Digital Safety education will be provided in the following ways:

- A planned e-safety programme provided as part of the Computer Science and also the PHSEE curricula at Key Stage 3 and registration sessions at Key Stage 4 and is regularly revisited
- Key e-safety messages that are reinforced as part of a planned programme of assemblies and presentations
- Rules for use of ICT systems are displayed on log-on screens
- Staff acting as good role models in their use of ICT, the internet and mobile devices
- Providing opportunities for students to be digital safety trainers for other users
- Embedding of Digital Literacy as part of the programmes of study in all subjects at all key stages so that students become
    - critically aware of the materials / content they access on-line and be guided to validate the accuracy of information
    - helped to understand the need for and purpose of the student AUA and encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school
    - taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet

Education & Training – Staff

It is essential that all staff receive digital safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A programme of e-safety training will be made available to staff. An audit of the training needs of all staff will be carried out regularly. (Some staff may identify e-safety as a training need within the performance management process).
- This Digital Safety policy and its updates will be presented to and discussed by staff in staff / team meetings / INSET days.
- The Digital Safety Lead will provide advice / guidance / training to individuals as required.
- Staff will be directed to relevant material addressing specific issues of digital and on-line safety

Training – Governors

Governors will be invited to take part in e-safety training/awareness sessions that may be offered in a number of ways:

- Attendance at training provided by the Local Authority , the National Governors Association and or other relevant organisation.
- Participation in school training / information sessions for staff or parents
- Participation in training activities arranged by student trainers

Education – parents / carers

Many parents and carers have only a limited understanding of e-safety risks and issues, yet they play an essential role in the education of their children and in the monitoring /

regulation of the children’s on-line experiences. The school will therefore seek to provide information and awareness to parents and carers through:

- Relevant information in Insight magazine
- Through the school website e-safety pages – including helpsheets, publications and updates of key e-safety issues and advice.
- Parent information evenings
- Providing opportunities for students to act as parent trainers\instructors in digital literacy

Technical – infrastructure / equipment, filtering and monitoring

The school will work to ensure:

- “appropriate filters and appropriate monitoring systems are in place. Children should not be able to access harmful or inappropriate material from the school or colleges IT system” however, schools will need to “be careful that “over blocking” does not lead to unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding.” (Keeping Children Safe in Education, 2019 (DfE))
- “children are safe from terrorist and extremist material when accessing the internet in school, including by establishing appropriate levels of filtering" (Revised Prevent Duty Guidance, 2015 (Home Office))
- the system of Unified Sign On from LGfL and the internal setup of LDAP that allows users access to school email, online school systems (including e-praise and SMHW, for students, and remote access, MINT and Room Booking Systems for staff) are correctly and effectively used, so that users are able to logon to the various systems with their own (unified) username and password that is linked to their status in the MIS (Sims.net).
- Users have clearly defined access rights to school ICT systems, including remote access. Details of the network access rights available to groups of staff users will be recorded in the permissions grid.
- The WebScreen filtering service is set up and managed to provide filtering for all internet access, including access through personal devices connected to the school’s wireless network.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (eg racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Digital Safety Lead arrange to temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.
- Servers, wireless systems and cabling are securely located and physical access restricted and appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, hand held devices etc from accidental or malicious attempts which might threaten the security of the school systems and data
- An agreed process is in place for the provision of temporary access of “guests” (eg trainee teachers, visitors) onto the school system.
- An agreed process is in place for the installation on the network of executable files and computer programs, for the saving of media files and other copyright material,

and for the storage of files and other material on users' home drives and shared network drives.

- Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured. (see GDPR documentation for further detail)
- The school infrastructure and individual workstations are protected by up to date virus software and that there is an appropriate and comprehensive back-up routine, with safe storage of back-up tapes and a disaster recovery plan.

Mobile Technologies including BYOD

Students in Years 7 to 11 are not allowed to use mobile phones in school. If a Year 7 to 11 student's mobile phone is seen or heard on the school site it will be confiscated and held for 7 days.

Staff and Sixth form students are permitted to have mobile devices in school (the rules around sixth form mobiles are established in the Sixth Form code of conduct). These users are able to connect to the school's WiFi network using their USO credentials. For mobile devices connected to the school's WiFi network the standard filtering and monitoring restrictions apply.

Where there is an agreed purpose, need and availability, students and\or staff may be loaned a mobile device (laptop or tablet) which may also be used at home as well as within school. These devices will be set up to ensure that appropriate filters and safeguards are in place to guard against misuse.

Use of digital and video images

When using and producing digital images or video, staff should educate students about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet eg on social networking sites.

- Staff and students are allowed to take digital / video images to support educational aims, but must follow school policies concerning the taking, sharing, distribution and publication of those images.
    - Care should be taken when taking digital / video images that students are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
    - Staff and students must not take, use, share, publish or distribute images of others without their permission
    - Photographs that include students intended for publication (on a website, or elsewhere) should be selected carefully and will comply with good practice guidance on the use of such images. Students' full names must not be associated with their image when published on-line.

Communications

When using communication technologies the school considers the following as good practice:

- The official school email service may be regarded as safe and secure. Staff and students should therefore use only the school email service to communicate with others when in school, or on school systems (eg by remote access).

- Users need to be aware that email communications may be monitored
- Users should immediately report, to a teacher (if a student) or their line manager or Digital Safety Lead, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.
- Any digital communication between staff and students or parents / must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or public chat / social networking programmes must not be used for these communications.
- Students will be taught about email safety issues, such as the risks attached to the use of personal details. They will also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material.

Fuller information on School Communications are available in the School Communications Protocol

Data Protection

Personal data will be recorded, processed, transferred and made available according to General Data Protection Regulations and the Data Protection Act 2018.

The school will ensure that it adheres to the seven key principles of GDPR

- Lawfulness, fairness and transparency
  - by ensuring there is a lawful basis for collecting and using personal data.
  - by ensuring no use of the data is in breach of any other laws.
  - by not processing the data in a way that is unduly detrimental, unexpected or misleading to the individuals concerned.
  - by being clear, open and honest about personal data is used.

- Purpose limitation
  - by being clear of the purposes for which data is processed and including this information within our Privacy notices and other documentation.
- Data minimisation
  - by ensuring that ensuring that the personal data held is limited to what is necessary
- Accuracy
  - by taking all reasonable steps to ensure the personal data we hold is up-to-date, accurate not neither misleading or in error
- Storage limitation
  - by retaining personal data only in accordance with our retention policy.
- Integrity and confidentiality
  - by having in place appropriate security measures to protect the personal data we hold
  - by having appropriate policies and practices to minimise the risks of data loss or data breach
- Accountability
  - by having appropriate measures and records in place to demonstrate our compliance with GDPR principles

Fuller information on Data Protection can be found in the school's Data Protection Policy and associated documents.

Unsuitable / inappropriate activities

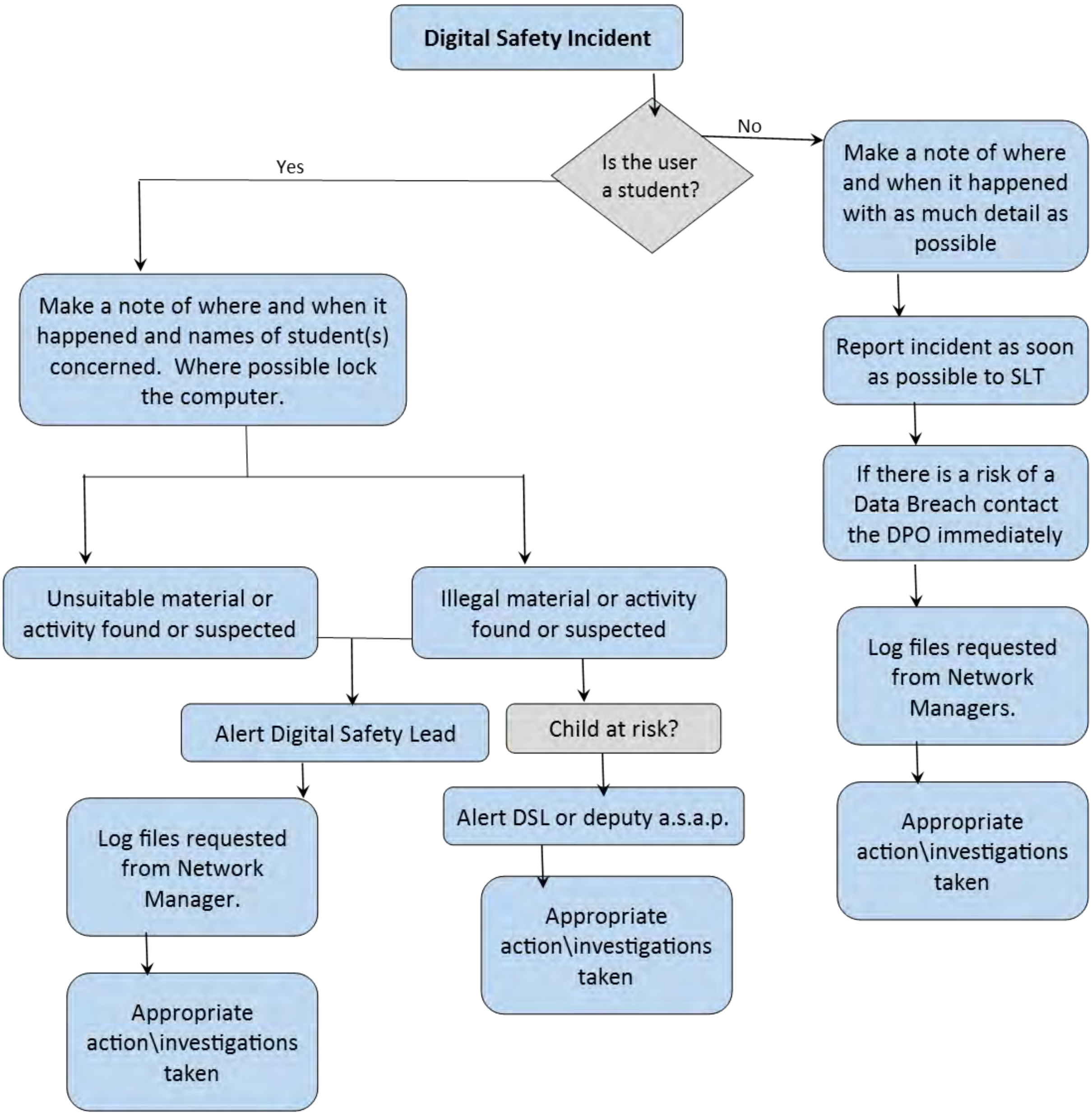
Some internet activity, eg accessing material that is illegal, would obviously be banned from school and all other ICT systems. Other activities eg Cyber-bullying could lead to criminal prosecution and would also be banned as a matter of course. There are however a range of activities which may, generally, be legal but would be inappropriate in a school context, either because of the age of the users or the nature of those activities.

The school believes that the activities referred to below are inappropriate in a school context and that users should not engage in these activities in school or outside school when using school equipment or systems except with the expressed permission of the Headteacher.

- Use of school systems to run a private business
- Creating of propagating viruses or malware
- Engaging in hacking or attempting to breach computer security settings
- Non-educational on-line gaming
- On-line gambling
- On-line trading
- File sharing that is in breach, or risks being in breach, of copyright and licensing agreements.

Responding to incidents of misuse

It is hoped that all members of the school community will be responsible users of ICT, who understand and follow this policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse. In these instance the processes outline in the flow chart below should be followed.


Digital Safety Incident
Is the user a student?
Yes
No
Make a note of where and when it happened and names of student(s) concerned. Where possible lock the computer.
Make a note of where and when it happened with as much detail as possible
Report incident as soon as possible to SLT
If there is a risk of a Data Breach contact the DPO immediately
Log files requested from Network Managers.
Appropriate action\investigations taken
Unsuitable material or activity found or suspected
Illegal material or activity found or suspected
Alert Digital Safety Lead
Child at risk?
Log files requested from Network Manager.
Alert DSL or deputy a.s.a.p.
Appropriate action\investigations taken
Appropriate action\investigations taken

Legislation

There is an extensive legislative framework that underpins this Digital Safety Policy, the key items are listed below.

Computer Misuse Act 1990

This Act makes it an offence to:

- Erase or amend data or programs without authority;
- Obtain unauthorised access to a computer;
- “Eavesdrop” on a computer;
- Make unauthorised use of computer time or facilities;
- Maliciously corrupt or erase data or programs;
- Deny access to authorised users.

Data Protection Act 2018

This protects the rights and privacy of individual’s data, providing the protections of the General Data Protection Regulations. This also requires organisations to respond very swiftly to any data breaches and also to respond effectively to Subject Access Requests for their personal data.

Freedom of Information Act 2000

The Freedom of Information Act gives individuals the right to request information held by public authorities. All public authorities and companies wholly owned by public authorities have obligations under the Freedom of Information Act. When responding to requests, they have to follow a number of set procedures.

Communications Act 2003

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.

Malicious Communications Act 1988

It is an offence to send an indecent, offensive, or threatening letter, electronic communication or other article to another person.

Regulation of Investigatory Powers Act 2000

It is an offence for any person to intentionally and without lawful authority intercept any communication. Monitoring or keeping a record of any form of electronic communications is permitted, in order to:

- Establish the facts;
- Ascertain compliance with regulatory or self-regulatory practices or procedures;
- Demonstrate standards, which are or ought to be achieved by persons using the system;
- Investigate or detect unauthorised use of the communications system;
- Prevent or detect crime or in the interests of national security;
- Ensure the effective operation of the system.
- Monitoring but not recording is also permissible in order to:
- Ascertain whether the communication is business or personal;
- Protect or support help line staff.
- The school reserves the right to monitor its systems and communications in line with its rights under this act.

Trade Marks Act 1994

This provides protection for Registered Trade Marks, which can be any symbol (words, shapes or images) that are associated with a particular set of goods or services. Registered Trade Marks must not be used without permission. This can also arise from using a Mark that is confusingly similar to an existing Mark.

Copyright, Designs and Patents Act 1988

It is an offence to copy all, or a substantial part of a copyright work. There are, however, certain limited user permissions, such as fair dealing, which means under certain circumstances permission is not needed to copy small amounts for non-commercial research or private study. The Act also provides for Moral Rights, whereby authors can sue if their name is not included in a work they wrote, or if the work has been amended in such a way as to impugn their reputation. Copyright covers materials in print and electronic form, and includes words, images, and sounds, moving images, TV broadcasts and other media (e.g. youtube).

Telecommunications Act 1984
It is an offence to send a message or other matter that is grossly offensive or of an indecent, obscene or menacing character. It is also an offence to send a message that is intended to cause annoyance, inconvenience or needless anxiety to another that the sender knows to be false.

Criminal Justice & Public Order Act 1994
This defines a criminal offence of intentional harassment, which covers all forms of harassment, including sexual. A person is guilty of an offence if, with intent to cause a person harassment, alarm or distress, they:

- Use threatening, abusive or insulting words or behaviour, or disorderly behaviour; or
- Display any writing, sign or other visible representation, which is threatening, abusive or insulting, thereby causing that or another person harassment, alarm or distress.

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.

Protection from Harrassment Act 1997
A person must not pursue a course of conduct, which amounts to harassment of another, and which he 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 is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

Protection of Children Act 1978
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 a 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). A person convicted of such an offence may face up to 10 years in prison

Sexual Offences Act 2003
A grooming offence 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) it is an offence to meet them or travel to meet them anywhere in the world 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, for your own gratification. 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, connexions staff fall in this category of trust). Any sexual intercourse with a child under the age of 13 commits the offence of rape.

Public Order Act 1986
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. Children, Families and Education Directorate page 38 April 2007.

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

Human Rights Act 1998
This does not deal with any particular issue specifically or any discrete subject area within the law. It is a type of “higher law”, affecting all other laws. In the school context, human rights to be aware of include:

- The right to a fair trial
- The right to respect for private and family life, home and correspondence
- Freedom of thought, conscience and religion
- Freedom of expression
- Freedom of assembly
- Prohibition of discrimination
- The right to education

These rights are not absolute. The school is obliged to respect these rights and freedoms, balancing them against those rights, duties and obligations, which arise from other relevant legislation.

The Education and Inspections Act 2006
Empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of students / pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour.

The Education and Inspections Act 2011
Extended the powers included in the 2006 Act and gave permission for Headteachers (and nominated staff) to search for electronic devices. It also provides powers to search for data on those devices and to delete data.

The Protection of Freedoms Act 2012
Requires schools to seek permission from a parent / carer to use Biometric systems

The School Information Regulations 2012
Requires schools to publish certain information on its website:

Serious Crime Act 2015
Introduced new offence of sexual communication with a child. Also created new offences and orders around gang crime (including CSE)

The Voyeurism Act 2019
This act outlaws “upskirting” (taking pictures under a person’s clothing without them knowing) where the purpose is to obtain sexual gratification or to cause humiliation, distress or alarm.