THE TOWERS

E SAFETY AND SAFE USE OF TECHNOLOGY POLICY

Approved by:	SLT – September 2019
Ownership:	Head, Head of ICT, Network Manager
Reviewed	September 2019
Next Review:	September 2020

The policy is applicable to all pupils including those in the Early Years Foundation Stage (EYFS).

Legal Status

This policy has been prepared with reference to:

- The Equality act 2010
- Early Years Foundation Stage 2017
- Prevent Strategy 2015 updated 2019
- Data Protection Act 2018

Related Documents

This policy should be read in conjunction with:

- SEND policy
- Behaviour Rewards and Sanctions Policy
- Child Protection and Safeguarding Policy
- Anti-Bullying Policy
- EYFS Policy
- Data Protection Policy
- Mobile Device Policy

Aims

We are committed to providing a caring, friendly and safe environment for all of our pupils so that they can learn in a secure atmosphere. This extends to the virtual environment. We are committed to safeguarding the well-being of our pupils whether they are on-line or using other multimedia technologies.

Contents

Introduction 3
Monitoring 4
Breaches 4
Incident Reporting 5
Student: The Towers E-Safety Agreement 6
E-Safety Agreement: Staff, Governors and Visitors 8
Computer Viruses 9
E-Mail 9
E-mailing Personal, Sensitive, Confidential or Classified Information 11
Equal Opportunities 11
E-Safety 11
E-Safety in the Curriculum: 12
E-Safety and Data Privacy Culture Skills Development for Staff 12
Managing the School E-Safety Messages 13
Incident Reporting, E-Safety Incident Log & Infringements 13
Complaints 13
Inappropriate Material 13
Flowchart to support decisions related to a non-illegal E-Safety incident: 15
Internet Access 16
Managing the Internet 16
Internet Us 16
Infrastructure 16
Managing Other Web Technologies 17
Parental Involvement 17
Passwords and Password Security 18
Password Security 18
Safe Use of Images 19
Consent of Adults Who Work at the School 20
Publishing Students' Images and Work 20
Storage of Images 20
Webcams 20
School ICT Equipment including Portable & Mobile ICT Equipment & Removable 21
Portable & Mobile ICT Equipment 21
Mobile Technologies 22
Social Media, including Facebook and Twitter 23
Telephone Services 24
Reviewing this Policy 24
Current Legislation 24

Introduction

ICT in the 21st Century is seen as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, schools need to build in the use of these technologies in order to arm our young people with the skills to access life-long learning and employment.

Information and Communications Technology covers a wide range of resources including; web based and mobile learning. It is also important to recognise the constant and fast paced evolution of ICT within our society as a whole. Currently the internet technologies children and young people are using both inside and outside of the classroom include:

- Websites
- E-mail, Instant Messaging and chat rooms
- Social Media, including Facebook and Twitter
- Mobile/ Smart phones with text, video and/ or web functionality
- Other mobile devices with web functionality
- Gaming, especially online
- Learning Platforms and Virtual Learning Environments
- Blogs and Wikis
- Podcasting
- Video Broadcasting
- Music Downloading

Whilst exciting and beneficial both in and out of the context of education, much ICT, 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 and that some have minimum age requirements, usually 13 years.

At The Towers, we understand the responsibility to educate our students on E- Safety issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.
The Towers holds personal data on learners, staff and other people to help them conduct their day-to-day activities. Some of this information is sensitive and could be used by another person or criminal organisation to cause harm or distress to an individual. The loss of sensitive information can result in

media coverage, and potentially damage the reputation of the school. This can make it more difficult for the school to use technology to benefit learners.

Everybody in the school has a shared responsibility to secure any sensitive information used in their day to day professional duties and even staff not directly involved in data handling should be made aware of the risks and threats and how to minimise them.

Both this policy and the Acceptable Use Agreement (for all staff, governors, visitors and students) are inclusive of both fixed and mobile internet; technologies provided by the school (such as PCs, laptops, mobile devices, webcams, whiteboards, voting systems, digital video equipment, etc.); and technologies owned by students and staff, but brought onto school premises (such as laptops, mobile phones, and other mobile devices). This also applies to devices used by staff for work at home purposes.

Monitoring

Authorised ICT staff may inspect any ICT equipment owned or leased by the school at any time without prior notice. If you are in doubt as to whether the individual requesting such access is authorised to do so, please ask for their identification badge and contact their department. Any ICT authorised staff member will be happy to comply with this request.

ICT authorised staff may monitor, intercept, access, inspect, record and disclose e-mails, instant messaging, internet/intranet use and any other electronic communications (data, voice or image) involving its employees or contractors, without consent, to the extent permitted by law. This may be to confirm or obtain school business related information; to confirm or investigate compliance with school policies, standards and procedures; to ensure the effective operation of school ICT; for quality control or training purposes; to comply with a Subject Access Request under the Data Protection Act 2018, or to prevent or detect crime.

ICT authorised staff may, without prior notice, access the e-mail or voice-mail account where applicable, of someone who is absent in order to deal with any business-related issues retained on that account.

All monitoring, surveillance or investigative activities are conducted by ICT authorised staff and comply with the Data Protection Act 2018, the Human Rights Act 1998, the Regulation of Investigatory Powers Act 2000 (RIPA) and the Lawful Business Practice Regulations 2000.

Please note that personal communications using School ICT may be unavoidably included in any business communications that are monitored, intercepted and/or recorded.

Breaches

A breach or suspected breach of policy by a school employee, contractor or student may result in the temporary or permanent withdrawal of school ICT hardware, software or services from the offending individual.
Any policy breach is grounds for disciplinary action in accordance with the school's procedures.

Breaches may also lead to criminal or civil proceedings.

The ICO's new powers to issue monetary penalties came into force on 25th May 2018, allowing the Information Commissioner's office to serve notices requiring organisations to pay a fine for serious breaches of the Data Protection Act 2018.

The data protection powers of the Information Commissioner's Office are to:

- Conduct assessments to check organisations are complying with the Act;
- Serve information notices requiring organisations to provide the Information Commissioner's Office with specified information within 72 hours of the breach being discovered;
- Serve enforcement notices and 'stop now' orders where there has been a breach of the Regulation, requiring organisations to take (or refrain from taking) specified steps in order to ensure they comply with the law;
- Prosecute those who commit criminal offences under the Act;
- Conduct audits to assess whether organisations processing of personal data follows good practice,
- Report to Parliament on data protection issues of concern

Incident Reporting

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported to the school's E-Safety Co-ordinator and Network Manager. Additionally, all security breaches, lost/stolen equipment or data (including remote access login information and PINs), virus notifications, unsolicited emails, misuse or unauthorised use of ICT and all other policy non-compliance must be reported to your E-Safety Co-ordinator and Network Manager.

Please refer to the section incident Reporting, E-Safety Incident Log & Infringements.

Student: The Towers E-Safety Agreement

- I will only use ICT systems in school, including the internet, e-mail, digital video and mobile technologies for school purposes.
- I will not download or install software on school technologies.
- I will only log on to the school network, other systems and resources with my own user name and password.
- I will follow the schools ICT security system and not reveal my passwords to anyone and change them regularly.
- I will only use my school e-mail address for school related purposes.
- I will make sure that all ICT communications with students, teachers or others is responsible and sensible.
- I will be responsible for my behaviour when using the Internet. This includes resources I access and the language I use.
- I will not deliberately browse, download, upload or forward material that could be considered offensive or illegal. If I accidentally come across any such material I will report it immediately to my teacher.
- I will not give out any personal information such as name, phone number or address. I will not arrange to meet someone unless this is part of a school project approved by my teacher.
- Images of students and/ or staff will only be taken, stored and used for school purposes in line with school policy and not be distributed outside the school network without the permission of the Head.
- I will ensure that my online activity, both in school and outside school, will not cause my school, the staff, students or others distress or bring into disrepute.
- I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset or offend any member of the school community
- I will respect the privacy and ownership of others' work on-line at all times.
- I will not attempt to bypass the internet filtering system.
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available to my teachers.
- I understand that these rules are designed to keep me safe and that if they are not followed, school sanctions will be applied and my parent /carer may be contacted.
- My parents/carers will supervise my internet research for school work at home

The Towers
Confidence & Education For Life

Dear Parent \ Carer

ICT including the internet, e-mail, mobile technologies and online resources have become an important part of learning in our school. We expect all students to be safe and responsible when using any ICT. It is essential that students are aware of E-Safety and know how to stay safe when using any ICT.

Students are expected to read and discuss the agreement attached with their parent or carer and then to sign and follow the terms of the agreement. Any concerns or explanation can be discussed with their class teacher or the school E-Safety coordinator.

Please return the bottom section of this form to school for filing.

✂

Student and Parent \ carer signature

We have discussed this document and …….. (Student name) agrees to follow the E-Safety rules and to support the safe and responsible use of ICT at The Towers.

Parent\ Carer Signature …….

Student Signature…….

Form …… Date ……

E-Safety Agreement:
Staff, Governors and Visitors Acceptable Use \ E-Safety Agreement \ Code of Conduct

ICT (including data) and the related technologies such as e-mail, the internet and mobile devices are an expected part of our daily working life in school. This agreement is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with the school E-Safety coordinator or Network Manager.

- I will only use the school's email \ Internet \ Virtual Learning Platform and any related technologies for professional purposes or for uses deemed 'reasonable' by the Head or Governing Body.
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities
- I will ensure that all electronic communications with students and staff are compatible with my professional role.
- I will not give out my own personal details, such as mobile phone number and personal e-mail address, to students.
- I will only use the approved, secure e-mail system(s) for any school business.
- I will ensure that personal data (such as data held on SIMS software) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Head or Governing Body. Personal or sensitive data taken off site must be encrypted.
- I will not install any hardware or software <u>without</u> permission of the School IT Department
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Images of students' and\or staff will only be taken on school owned equipment, stored and used for professional purposes in line with school policy and with written consent of the parent, carer or staff member. Images will not be distributed outside the school network without the permission of the parent/ carer, member of staff or Head.
- I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset or offend any member of the school community
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to my Line Manager or Head.
- I will respect copyright and intellectual property rights.
- I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.
- I will support and promote the school's e-Safety and Data Security policies and help students to be safe and responsible in their use of ICT and related technologies.
- I understand this forms part of the terms and conditions set out in my contract of employment.
- Any loss of data or potential data breach should be reported as soon as possible to the Data Protection Officer.
- I give permission for my mobile device to be confiscated and accessed for investigation purposes in the event of any safeguarding concern.

User Signature

I agree to follow this code of conduct and to support the safe and secure use of ICT throughout the school

Signature …….…… Date ……

Full Name …….... (Printed) Job title . . . . . .

Computer Viruses

- All files downloaded from the Internet, received via e-mail or on removable media such as a memory stick, are automatically checked for any viruses using school provided antivirus software before being used (Removable media is automatically scanned when connected to a school computer)
- Never interfere with any anti-virus software installed on school ICT equipment that you Use.
- If your machine is not routinely connected to the school network, you must make provision for regular virus updates through the IT Department

If you suspect there may be a virus on any school ICT equipment, stop using the equipment and contact the IT Department immediately. The IT Department will advise you what actions to take and be responsible for advising others that need to know

E-Mail

The use of e-mail within most schools is an essential means of communication for both staff and students. In the context of school, e-mail should not be considered private. Educationally, e-mail can offer significant benefits including; direct written contact between schools on different projects, be they staff based or student based, within school or international. We recognise that students need to understand how to style an e-mail in relation to their age and good network etiquette; 'netiquette'.

Managing e-Mail

- The school gives all staff their own e-mail account to use for all school business as a work based tool. This is to protect staff, minimise the risk of receiving unsolicited or malicious e- mails and avoids the risk of personal profile information being revealed
- It is the responsibility of each account holder to keep the password secure. For the safety and security of users and recipients, all mail is filtered and archived; if necessary e-mail histories can be traced. The school email account should be the account that is used for all school business
- Under no circumstances should staff contact students, parents or conduct any school business using personal e-mail addresses
- The school requires a standard disclaimer to be attached to all e-mail correspondence, stating that, 'the views expressed are not necessarily those of the school. This disclaimer is automatically added to any school email that is sent
- All e-mails should be written and checked carefully before sending, in the same way as a letter written on school headed paper
- Staff sending e-mails to external organisations, parents or students are advised to cc. the Head, line manager or appropriate colleague where appropriate

- Students may only use school approved accounts on the school system and only under direct teacher supervision for educational purposes
- E-mails created or received as part of your school job will be subject to disclosure in response to a subject data request for information under the Data Protection Act 2018.
  You must therefore actively manage your e-mail account as follows:
- ➢ Delete all e-mails of short-term value
- ➢ Organise e-mail into folders and carry out frequent house-keeping on all folders and archives
- All students have their own individual school issued accounts
- The forwarding of chain letters is not permitted in school. However the school has set up an account (websupport@thetowersschool.org) to allow students to forward any chain letters causing them anxiety. No action will be taken with this account by any member of the school community other than the Network Manager and IT Support Department.
- All student e-mail users are expected to adhere to the generally accepted rules of netiquette particularly in relation to the use of appropriate language and not revealing any personal details about themselves or others in e-mail communication, or arrange to meet anyone without specific permission, virus checking attachments
- Students must immediately tell a teacher\ trusted adult if they receive an offensive e-mail
- Staff must inform (the E-Safety co-ordinator\ Network manager) if they receive an offensive e-mail
- Students are introduced to e-mail as part of the ICT Scheme of Work
- However you access your school e-mail (whether directly, through webmail when away from the office or on non-school hardware) all the school e-mail policies apply and must only be viewed by school members.
- Where staff link personal devices to school email, the device must be password protected to block unauthorised access to the device. Any notifications of new e-mails when the device is locked, must not show the subject of the e-mail

Sending e-Mails

- If sending e-mails containing personal, confidential, classified or financially sensitive data to external third parties or agencies, refer to the Section E-mailing Personal, Sensitive, Confidential or Classified Information
- Use your own school e-mail account so that you are clearly identified as the originator of a message
- Keep the number and relevance of e-mail recipients, particularly those being copied, to the minimum necessary and appropriate
- Do not send or forward attachments unnecessarily. Whenever possible, send the location path to the shared drive rather than sending attachments
- School e-mail is not to be used for personal advertising

Receiving e-Mails

- Check your e-mail regularly
- Activate your ‘out-of-office’ notification when away for extended periods
- Never open attachments from an untrusted source; Consult the IT Department first
- Do not use the e-mail systems to store attachments. Detach and save business related work to the appropriate shared drive\folder
- The automatic forwarding and deletion of e-mails is not allowed

E-mailing Personal, Sensitive, Confidential or Classified Information

Where your conclusion is that an external e-mail must be used to transmit such data:

Obtain express consent from the Head or Assistant Head Academic\Pastoral to provide the information by e-mail. Exercise caution when sending the e-mail and always follow these checks before releasing the e-mail:

- Password protect
- Use SIMS to log sensitive data and notify staff of this log via the SIMS messaging
- Verify the details, including accurate e-mail address, of any intended recipient of the information
- Verify (by phoning) the details of a requestor before responding to e-mail requests for information
- Do not copy or forward the e-mail to any more recipients than is absolutely necessary
- Do not send the information to anybody/person whose details you have been unable to separately verify (usually by phone)
- Send the information as a password protected encrypted document **attached** to an email
- Provide the password & encryption keys in **separate** e-mails with the recipient(s)
- Do not identify such information in the subject line of any e-mail
- Request confirmation of safe receipt

Where required or requested staff will follow procedures as requested by external partners for sharing confidential data such as Child Protection issues and or personal information.

Equal Opportunities

Students with Additional Needs:
The school endeavours to create a consistent message with parents for all students and this in turn should aid establishment and future development of the school's E-Safety rules.

However, staff are aware that some students may require additional support or teaching including adapted resources, reminders, prompts and further explanation to reinforce their existing knowledge and understanding of E-Safety issues.

Where a student has poor social understanding, careful consideration is given to group interactions when raising awareness of E-Safety. Internet activities are planned and well managed for these children and young people.

E-Safety

E-Safety - Roles and Responsibilities:

As E-Safety is an important aspect of strategic leadership within the school, the Head and Governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. The named E-Safety co-ordinators in this school is are the Assistant Head's Academic and Pastoral who have been designated this role as a members of the senior leadership team. All members of the school community have been made aware of who holds this post. It is the role of the E-Safety Coordinators to

keep abreast of current issues and guidance through organisations such as WSCC, CEOP (Child Exploitation and Online Protection) and Childnet.

Senior Management and governors are updated by the Head \ E-Safety co-ordinators and all governors have an understanding of the issues and strategies at our school in relation to local and national guidelines and advice.

This policy for staff, governors, visitors and students, is to protect the interests and safety of the whole school community. It is linked to the following mandatory school policies: child protection, health and safety, home–school agreements, and behaviour\student discipline (including the anti-bullying) policy and Life Long Learning

E-Safety in the Curriculum:

ICT and online resources are increasingly used across the curriculum. We believe it is essential for E-Safety guidance to be given to the students on a regular and meaningful basis. E-Safety is embedded within our curriculum and we continually look for new opportunities to promote E-Safety.

- The school provides opportunities within a range of curriculum areas to teach about E-Safety
- Educating students about the online risks that they may encounter outside school is done informally when opportunities arise and as part of the E-Safety curriculum
- Students are aware of the relevant legislation when using the internet such as data protection and intellectual property which may limit what they want to do but also serves to protect them
- Students are taught about copyright, respecting other people's information, safe use of images and other important areas through discussion, modelling and appropriate activities
- Students are made aware of the impact of Cyberbullying and know how to seek help if they are affected by any form of online bullying. Students are also aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent \ carer, teacher \ trusted staff member, or an organisation such as Cybermentors, Childline or CEOP report abuse button.
- Staff and students can access Internet Safety advice on the VLE:

  https://thetowersschool.fireflycloud.net/internet-safety

  including the CEOP report abuse link: ***https://www.ceop.police.uk/Ceop-Report/***

- Students are taught to critically evaluate materials and learn good searching skills through cross curricular teacher models, discussions and via the ICT curriculum and Life Long Learning lessons

E-Safety and Data Privacy Culture Skills Development for Staff

- Our staff receive regular information and training on E-Safety and how they can promote the 'Stay Safe' online messages in the form of CPD and regular updates via email.
- New staff receive information on the school's Acceptable use and safety policy as part of their induction
- All staff have been made aware of their individual responsibilities relating to the safeguarding of children within the context of E-Safety and know what to do in the event of misuse of technology by any member of the school community (see enclosed flowcharts)
- All staff are encouraged to incorporate E-Safety activities and awareness within their curriculum areas

Managing the School E-Safety Messages

- We endeavour to embed E-Safety messages across the curriculum whenever the internet and/or related technologies are used
- The E-Safety policy will be introduced to new students at the start of each school year with key aspects highlighted annually to all students
- Students starting at The Towers mid-year will undergo catch-up sessions
- E-Safety posters will be prominently displayed
- The key E-Safety advice will be promoted widely through school displays, newsletters and curriculum activities

Incident Reporting, E-Safety Incident Log & Infringements

Incident Reporting E-Safety Incident Log

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported to the school's Network Manager, E-Safety Coordinator and Data Protection Officer. Additionally, all security breaches, lost/stolen equipment or data (including remote access login information and PINs), virus notifications, unsolicited emails, misuse or unauthorised use of ICT and all other policy non-compliance must be reported to your Network Manager, E-Safety Co-ordinator and Data Protection Officer.

Misuse and Infringements:

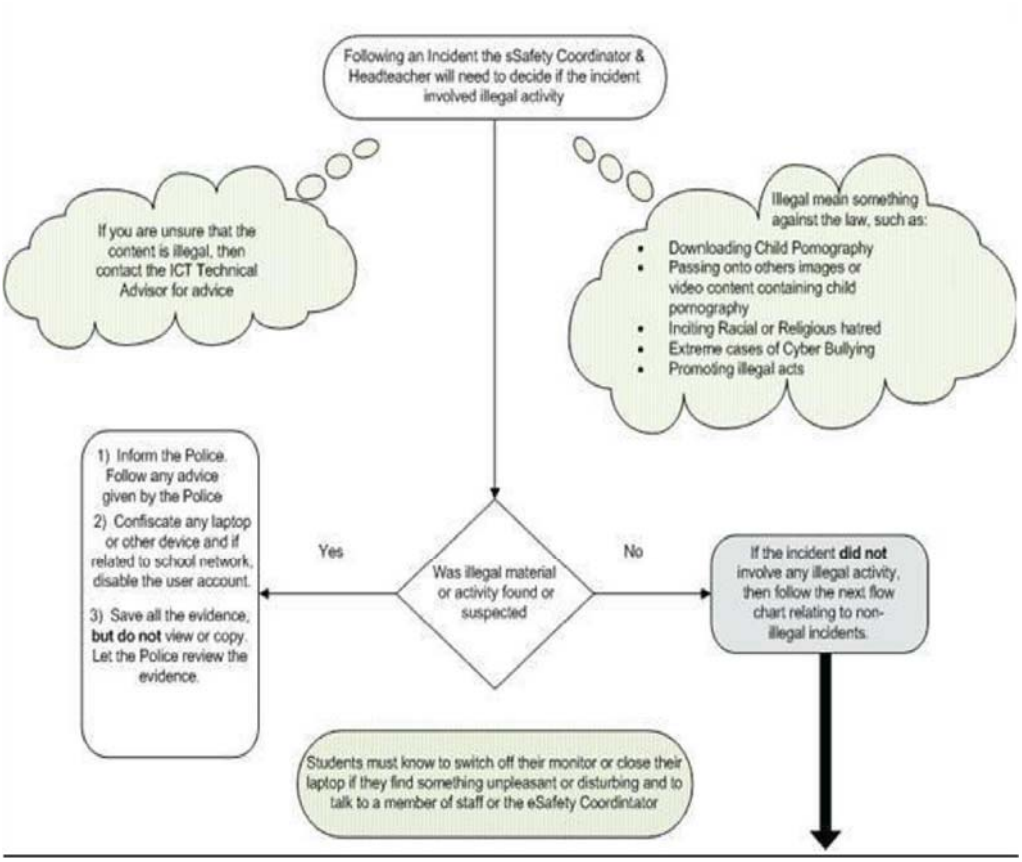
Complaints

Complaints and\ or issues relating to E-Safety should be made to the E-Safety co-ordinator or Head. Incidents should be logged and the **Flowcharts for Managing an E-Safety Incident** should be followed.

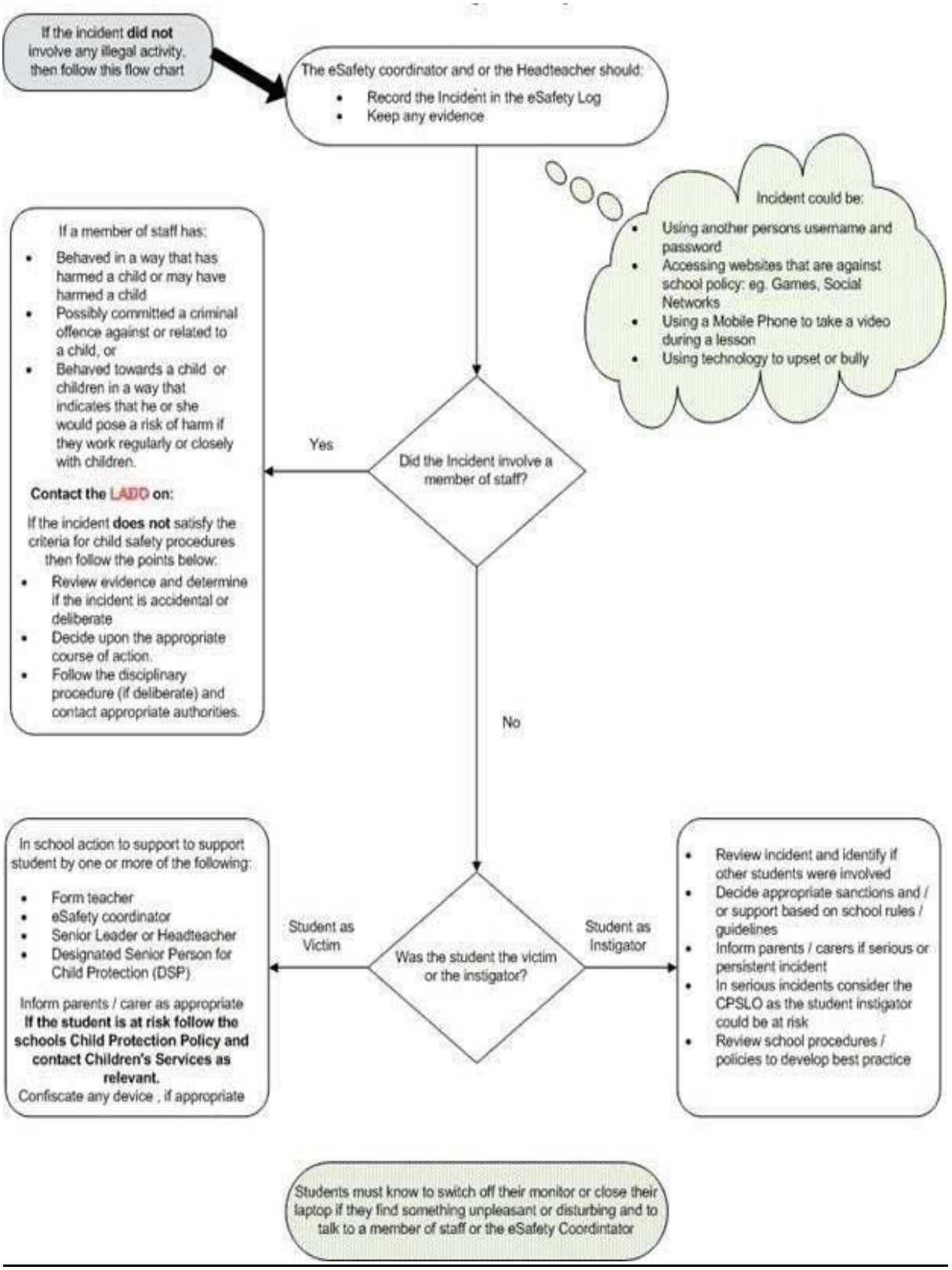
Inappropriate Material

- All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the E-Safety co-ordinator
- Deliberate access to inappropriate materials by any user will lead to the incident being logged by the E-Safety co-ordinator, depending on the seriousness of the offence; investigation by the Head, immediate suspension, possibly leading to dismissal and involvement of police for very serious offences (see flowchart)
- Users are made aware of sanctions relating to the misuse or misconduct by an interview with an SLT member and also by letter.

Flowcharts for Managing an E-Safety Incident



Flowchart to support decisions related to a non-illegal E-Safety incident:



Internet Access

The internet is an open worldwide communication medium, available to everyone at all times. Anyone can view information, send messages, discuss ideas and publish material which makes it both an invaluable resource for education, business and social interaction, as well as a potential risk to young and vulnerable people. All use of the **School Internet Service** is logged and the logs are randomly but regularly monitored. Whenever any inappropriate use is detected it will be followed up.

Managing the Internet

- The school provides students with supervised access to Internet resources (where reasonable) through the school's fixed and mobile internet connectivity
- Staff will preview any recommended sites before use
- Raw image searches are discouraged when working with students
- If Internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher. It is advised that parents recheck these sites and supervise this work. Parents will be advised to supervise any further research
- All users must observe software copyright at all times. It is illegal to copy or distribute school software or illegal software from other sources
- All users must observe copyright of materials from electronic resources

Internet Use

- You must not post personal, sensitive, confidential or classified information or disseminate such information in any way that may compromise the intended restricted audience
- Do not reveal names of colleagues, students, others or any other confidential information acquired through your job on any social networking site or other online application
- On-line gambling or gaming is not allowed

Infrastructure

- The Towers has an internal monitoring solution powered by a Sophos UTM Security Appliance where web-based activity is monitored and recorded.
- School internet access is controlled through the Sophos UTM web filtering service.
- The Towers web-filtering is the responsibility of IT Support Department
- The Towers is aware of its responsibility when monitoring staff communication under current legislation and takes into account; Data Protection Act 2018, The Telecommunications (Lawful Business Practice) (Interception of Communications)
  Regulations 2000, Regulation of Investigatory Powers Act 2000, Human Rights Act 1998
- Staff and students are aware that school based email and internet activity can be monitored and explored further if required
- The school uses management control tools for controlling and monitoring workstations
- If staff or students discover an unsuitable site, the screen must be switched off\ closed and the incident reported immediately to the e-safety coordinator teacher or IT Support Department as appropriate.
- It is the responsibility of the school, by delegation to the IT Department, to ensure that anti-virus protection is installed and kept up-to-date on all school machines

- Students and Staff using personal removable media are responsible for measures to protect against viruses, for example making sure that additional systems used have up-to-date virus protection software. It is not the school's responsibility nor the IT Departments to install or maintain virus protection on personal systems. (If students wish to bring in work on removable media it must be given to the Teacher or the IT Department for a safety check first when possible, although school pcs will automatically scan any device plugged in.)
- Students and staff are not permitted to download programs or files on school based technologies without seeking prior permission from head of the ICT Subject leader or the IT Department
- If there are any issues related to viruses or anti-virus software, the IT Department should be informed immediately by the member of staff in charge of the class at the time or by the member of staff using the computer. The IT department can be contacted via the IT Support Helpdesk on the VLE, email, or by phoning extension 219 during lessons.
- Where ever possible students using personal electronic storage devices must make sure they have a backup copy of any data on their school account. The Towers is not responsible for any data or coursework\ Controlled Assessment lost due to the failure of a personal electronic storage device.

Managing Other Web Technologies

Online technologies, including social networking sites, if used responsibly both outside and within an educational context can provide easy to use, creative, collaborative and free facilities. However it is important to recognise that there are issues regarding the appropriateness of some content, contact, culture and commercialism. To this end, we encourage our students to think carefully about the way that information can be added and removed by all users, including themselves, from these sites.

- At present, the school endeavours to deny access to social networking and online games websites to students within school
- All students are advised to be cautious about the information given by others on such websites, for example users not being who they say they are
- Students are taught to avoid placing images of themselves (or details within images that could give background details) on such websites and to consider the appropriateness of any images they post due to the difficulty of removing an image once online
- Students are always reminded to avoid giving out personal details on websites which may identify them or where they are (full name, address, mobile\home phone numbers, school details, IM\ email address, specific hobbies\interests)
- Our students are advised to set and maintain their online profiles to maximum privacy and deny access to unknown individuals
- Students are encouraged to be wary about publishing specific and detailed private thoughts and information online
- Our students are asked to report any incidents of Cyberbullying to the school
- Staff may only create blogs, wikis or other online areas in order to communicate with students using the school learning platform or other systems approved by the Head.

Parental Involvement

We believe that it is essential for parents\carers to be fully involved with promoting E-Safety both in and outside of school and to be aware of their responsibilities. We regularly consult and discuss E- Safety

with parents\ carers and seek to promote a wide understanding of the benefits of new technologies together with the associated risks.

- Parents\carers are asked to read through and sign acceptable use agreements on behalf of their child on admission to the school
- Parents\carers are required to make a decision as to whether they consent to images of their child being taken and used in the public domain (e.g., on school website)
- Parents\carers are expected to sign the E-Safety agreement on joining the school containing the following statement.
- "We will support the school approach to on-line safety and not deliberately upload or add any text, image, sound or video that could upset or offend any member of the school community"
- The school disseminates information to parents relating to E-Safety where appropriate in the form of:
    - Information and celebration evenings
    - Practical training sessions e.g. How to adjust the Facebook privacy settings
    - Posters
    - School website and newsletter items

Passwords and Password Security

Passwords

- **Always use your own** personal passwords.
- Make sure you enter your personal passwords each time you logon. Do not include passwords in any automated logon procedures.
- Staff should change temporary passwords at first logon.
- Change passwords whenever there is any indication of possible system or password compromise.
- Do not record passwords or encryption keys on paper or in an unprotected file.
- **Only disclose your personal password to authorised IT support staff when necessary, and never to anyone else.** Ensure that all personal passwords that have been disclosed are changed once the requirement is finished.
- **Never tell a child or colleague your password.**
- **If you are aware of a breach of security with your password or account inform the IT Department immediately**
- Passwords must contain a minimum of eight characters and be difficult to guess.
- Passwords should contain a mixture of upper and lowercase letters, numbers and symbols
- User ID and passwords for staff and students who have left the school are disabled from the system within 24 hours.

If you think your password may have been compromised or someone else has become aware of your password report this to the IT department

Password Security

Password security is essential for staff, particularly as they are able to access and use student data.

Staff are expected to have secure passwords, which are not shared with anyone. The students are expected to keep their passwords private and not to share with others, particularly their friends. Staff and students are regularly reminded of the need for password security.

- All users read and sign an Acceptable Use Agreement to demonstrate that they have understood the school's E-Safety Policy and Data Security.
- Users are provided with an individual network/email, learning platform and **M**anagement **I**nformation **S**ystem (where appropriate) log-in username. They are also expected to use a personal password and keep it private.
- Students are not allowed to deliberately access on-line materials or files on the school network, of their peers, teachers or other students.
- Staff are aware of their individual responsibilities to protect the security and confidentiality of the school networks, MIS systems and/or learning platform, including ensuring that passwords are not shared and are changed periodically. Individual staff users must also make sure that workstations are not left unattended and are locked.
- Due consideration should be given when logging into the school learning platform, virtual learning environment or other online application to the browser/cache options (shared or private computer).
- In our school, all ICT password policies are the responsibility of the IT Services Manager and all staff and students are expected to comply with the policies at all times.
- User's passwords will be changed on a termly basis. This will be an automatic procedure initiated via the school servers and where possible will be at the beginning of a term.

Staff are responsible for changing their logon on a termly basis in line with their user password changes.

Safe Use of Images

Taking of Images and Film
Digital images are easy to capture, reproduce and publish and, therefore, misuse. We must remember that it is not always appropriate to take or store images of any member of the school community or public, without first seeking consent and considering the appropriateness.

- Unless consent is withdrawn by parents on receipt of letter from the Head (on behalf of students) and staff, the school permits the appropriate taking of images by staff and students with school equipment.
- Staff are not permitted to use personal digital equipment, such as mobile phones and cameras, to record images of students, this includes when on field trips. However with the express permission of the Head, images can be taken provided they are transferred immediately and solely to the School's network and deleted from the staff device.
- Students are not permitted to use personal digital equipment, including mobile phones and cameras, to record images of students, staff and others without advance permission from the Head.
- Students and staff must have permission from the Head before any image can be uploaded for publication.
- All students and staff have the right to request removal/deletion of images or video content containing themselves.

Consent of Adults Who Work at the School

- Permission to use images of all staff who work at the school is sought on induction and a copy is located in the personnel file.

Publishing Students' Images and Work

On a child's entry to the school, unless consent is withdrawn by parents on receipt of letter from the Head (on behalf of students) and staff, student images and work may be used in the following ways:

- On the school web site.
- In the school prospectus and other printed publications that the school may produce for promotional purposes.
- Recorded/ transmitted on a video or webcam.
- On the school's learning platform or Virtual Learning Environment.
- In display material that may be used in the school's communal areas.
- In display material that may be used in external areas, i.e. exhibition promoting the school.
- General media appearances, e.g. local/ national media/ press releases sent to the press highlighting an activity (sent using traditional methods or electronically).

This consent form is considered valid for the entire period that the child attends this school unless there is a change in the child's circumstances where consent could be an issue, e.g. divorce of parents, custody issues, etc.

Parents, carers or students may withdraw permission, in writing, at any time

Students' names will not be published alongside their image and vice versa. E-mail and postal addresses of students will not be published. Students' full names will not be published.

Before posting student work on the Internet, a check needs to be made to ensure that permission has been given for work to be displayed.

Only the designated staff member for the relevant Web section has authority to upload to the site.

Storage of Images

- Images/ films of children are stored on the school's network and maybe stored on third party cloud storage (i.e. Office 365)
- Students and staff are not permitted to use personal portable electronic media for storage of images (e.g. USB sticks) without the express permission of the Head or E Safety coordinator
- Rights of access to this material are restricted to the teaching staff and students within the confines of the school network or other online school resource
- The IT Department and the Data Protection Officer has the responsibility of deleting the images when they are no longer required.

Webcams

- We do not use publicly accessible webcams in school

- Webcams in school are only ever used for specific learning purposes, i.e. monitoring hens' eggs and never using images of children or adults
- Misuse of the webcam by any member of the school community will result in sanctions (as listed under the ' inappropriate materials' section of this document)
- Webcams can be requested from the IT Support department. Notification is given in the area(s) filmed by webcams by signage.
- Consent is sought from parents/carers and staff on joining the school, in the same way as for all images.

School ICT Equipment including Portable & Mobile ICT Equipment & Removable Media

School ICT Equipment

- As a user of the school ICT equipment , you are responsible for your activity
- There is a record of all school IT devices. Serial numbers are recorded as part of the school's inventory.
- Visitors are not allowed to plug their ICT hardware into the school network points (unless special provision has been made). They should be directed to the Guest Wireless Network. The code for which is kept at the main reception desk.
- Staff must ensure that all ICT equipment that is used is kept physically secure
- Do not attempt unauthorised access or make unauthorised modifications to computer equipment, programs, files or data. This is an offence under the Computer Misuse Act 1990
- It is imperative that you save your data on a frequent basis to the school network. You are responsible for the backup and restoration of any of your data that is not held on the school's network.
- Personal or sensitive data should not be stored on the local drives of desktop PC, laptop, USB memory stick, or other portable electronic device. If it is necessary to do so, you must use the encryption software for portable electronic devices recommended by the school
- It is recommended that a time locking screensaver is applied to all machines. Any device accessing personal data must have a locking screensaver as must any user profiles
- Privately owned ICT equipment should not be used on a school network without checks for compliancy with the schools network security.
- On termination of employment, resignation or transfer, return all ICT equipment to your IT Manager. You must also provide details of all your system logons so that they can be disabled
- It is your responsibility to ensure that any information accessed from your own PC or removable media equipment is kept secure, and that no personal, sensitive, confidential or classified information is disclosed to any unauthorised person
- All ICT equipment allocated to staff must be authorised by the appropriate Line Manager. Authorising Managers are responsible for:
    - Maintaining control of the allocation and transfer within their department.
    - Recovering and returning equipment when no longer needed.

- All redundant ICT equipment is disposed of in accordance with Waste Electrical and Electronic Equipment (WEEE) directive and Data Protection Act 2018

Portable & Mobile ICT Equipment

This section covers such items as laptops, mobile devices and removable data storage devices. Please refer to the relevant sections of this document when considering storing or transferring personal or sensitive data

- All activities carried out on school systems and hardware will be monitored in accordance with the general policy
- Staff must ensure that all school data is stored on the school network, and must not be stored on a laptop. Any equipment where personal data is likely to be stored must be encrypted
- Equipment must be kept physically secure in accordance with this policy to be covered for insurance purposes. When travelling by car, best practice is to place the laptop in the boot of your car before starting your journey
- Synchronise all locally stored data, including diary entries, with the central school network server on a frequent basis
- Ensure portable and mobile ICT equipment is made available as necessary for anti-virus updates and software installations, patches or upgrades
- The installation of any applications or software packages must be authorised by the IT Department, fully licensed and only carried out by the IT Department

Mobile Technologies

Many emerging technologies offer new opportunities for teaching and learning including a move towards personalised learning and 1:1 device ownership for children and young people. Mobile technologies such as, Smartphones, Tablets, games players are generally very familiar to children outside of school. They often provide a collaborative, well-known device with possible internet access and thus open up risk and misuse associated with communication and internet use. Emerging technologies will be examined for educational benefit and the risk assessed before use in school is allowed. The Towers chooses to manage the use of these devices in the following ways so that users exploit them appropriately:

Personal Mobile Devices (including phones)

- The school allows staff to bring in personal mobile phones and devices for their own use. Under no circumstances does the school allow a member of staff to contact a student or parent/ carer using their personal device
- Students are allowed to bring personal mobile devices/phones to school but must follow the schools guidance on the use of mobile phones
- This technology may be used for educational purposes, as mutually agreed with the Head. The device user, in this instance, must always ask the prior permission of the bill payer

- The school is not responsible for the loss, damage or theft of any personal mobile device

- The sending of inappropriate text messages between any members of the school community is not allowed.
- Permission must be sought before any image or sound recordings are made on these devices of any member of the school community
- Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device

- When using personal devices for e-mail, follow the guidance on page 11

School Provided Mobile Devices (including phones)

- The sending of inappropriate text messages between any member of the school community is not allowed
- Permission must be sought before any image or sound recordings are made on the devices of any member of the school community
- Where the school provides mobile technologies such as phones, laptops and tablets for offsite visits and trips, only these devices should be used
- Where the school provides a laptop for staff, only this device may be used to conduct school business outside of school

Removable Media, Such as Portable Electronic Devices

- Always consider if an alternative solution already exists
- Only use recommended removable media
- Encrypt and password protect
- Store all removable media securely
- Removable media must be disposed of securely by IT Department

Social Media, including Facebook and Twitter

Facebook, Twitter and other forms of social media are increasingly becoming an important part of our daily lives.

- The Towers uses the school website, VLE, SchoolComms, Facebook and Twitter to communicate with students, parents and carers. The school staff authorised by the E-Safety committee are responsible for all postings on these technologies
- Staff ***are not*** permitted to access their personal social media accounts using school equipment at ***any time during lessons.***
- Students are not permitted to access their social media accounts whilst at school, using any school devices.

- Students are permitted to access their personal social media account using their own device (i.e. mobile phone) outside of lessons in accordance with the school guidance on use of mobile phones

- Staff, governors, students, parents and carers are regularly provided with information on how to use social media responsibly and what to do if they are aware of inappropriate use by others
- Staff, governors, students, parents and carers are aware that the information, comments, images and video they post online can be viewed by others, copied and stay online forever
- Staff, governors, students, parents and carers are aware that their online behaviour should at all times be compliant with UK law

Telephone Services

Mobile Phones
Staff are responsible for the security of school mobile phones, when issued to them for School trips etc. Always set the PIN code on the school mobile phone and do not leave it unattended and on display (especially in vehicles)

- Report the loss or theft of any school mobile phone equipment immediately
- The school remains responsible for all call costs until the phone is reported lost or stolen
- You must read and understand the user instructions and safety points relating to the use of your school mobile phone prior to using it
- School SIM cards must only be used in school provided mobile phones
- All school mobile phones are barred from calling premium rate numbers
- You must not send text messages to premium rate services
- In accordance with the **Finance policy** on the private use of school provided mobiles, you must reimburse the school for the cost of any personal use of your school mobile phone. This includes call charges incurred for incoming calls whilst abroad. Payment arrangements should be made through the finance administrator.
- Never use a hand-held mobile phone whilst driving a vehicle. Only genuine 999 or 112 (in Europe) emergency calls may be made if it would be unsafe to stop before doing so

Reviewing this Policy

- Staff and governors will be involved in reviewing the Policy on an annual basis
- The policy will be amended if new technologies are adopted or Central Government change the orders or guidance in any way

  There will be on-going opportunities for staff to discuss with the E-Safety coordinator any E-Safety issue that concerns them.

Current Legislation

Acts Relating to Monitoring of Staff email

Data Protection Act 2018
The Act requires anyone who handles personal information to comply with important data protection principles when treating personal data relating to any living individual. The Act grants individuals rights of access to their personal data, compensation and prevention of processing.
http://www.legislation.gov.uk/ukpga/2018/12/contents

The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
http://www.legislation.gov.uk/uksi/2000/2699/cont ents/made

Regulation of Investigatory Powers Act 2000
Regulating the interception of communications and making 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.

http://www.hmso.gov.uk/acts/acts2000/20000023.htm

Human Rights Act 1998 http://www.hmso.gov.uk/acts/acts1998/19980042.htm

Other Acts Relating to E-Safety
Racial and Religious Hatred Act 2006
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.

Sexual Offences Act 2003
The new 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. Schools should already have a copy of "*Children & Families: Safer from Sexual Crime*" document as part of their child protection packs. For more information: www.teachernet.gov.uk

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.

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 another person's password to access files)
- unauthorised access, as above, in order to commit a further criminal act (such as fraud)
- impair the operation of a computer or program

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

Malicious Communications Act 1988 (section 1)

This legislation makes it a criminal offence to send an electronic message (e-mail) 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.

Copyright, Design and Patents Act 1988
Copyright is the right to prevent others from copying or using work without permission. 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. Copyright infringement is to copy all or a substantial part of anyone's work without obtaining them 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.

Protection of Children Act 1978 (Section 1)
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). A person convicted of such an offence may face up to 10 years in prison.

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 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.

Acts Relating to the Protection of Personal Data Protection Order
2012
http://www.legislation.gov.uk/uksi/2012/1978/contents/made

The Freedom of Information Act 2005
http://www.ico.gov.uk/for_organisations/freedom_of_information_guide.aspx

Bibliography

http://www.childnet.com/resources
http://www.westsussexscb.org.uk/professionals/concerns-at-work-2/lado-local-authoritydesignated-officer/
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/439598/prevent-duty-departmental-advice-v6.pdf