Online safety, IT and Acceptable Use Policy

Contents:

Last Updated by SC April 2024
Further update by AB 04/04/2024

Date of next review Summer 2025

Policy Scope

This policy applies to all members of the school community (including staff, pupils, volunteers, parents, guardians and visitors) who have access to and are users of Tring Park ICT systems, both in and out of school.

The Education and Inspections Act 2006 empowers Head Teachers, 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. 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 is linked to membership of the school.

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / guardians of incidents of inappropriate e-safety behaviour that take place in and out of school.

Policy Objectives

At Tring Park School, we understand the responsibility to educate our pupils 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 principle objectives are that:

- All governors, teachers, teaching assistants and support staff will have an understanding of what E-safety, acceptable ICT use and radicalisation are and why we need to be vigilant in school

- All governors, teachers, teaching assistants and support staff will know what the school policy is on E-safety, acceptable ICT use and anti-radicalisation and will follow the policy

- All parents and students will know that the school has policies in place to keep students safe from harm, and that the school regularly reviews its systems to ensure they are appropriate and effective

The main aims of this policy are to ensure that staff are fully engaged in being vigilant about E-safety, grooming and radicalisation; that they overcome professional disbelief that such issues will not happen here, and that they ensure that we work alongside other professional bodies and agencies to ensure that our students are safe from harm.

Related safeguarding documents, policies and procedures:

As safeguarding is a priority across all areas of the school, this policy should not be read alone but in conjunction with the documents, policies and procedures listed below. This is not a definitive list as the school is committed to reviewing and extending its safeguarding provision continuously. However, the list encompasses all the areas in which links are clearly made and the safety of pupils actively promoted.

- Safeguarding Children Quick Reference Guide
- Staff handbook
- Pupil handbooks
- Parent handbooks
- Departmental handbooks
- Safer recruitment policy and procedures
- Procedures for managing allegations against staff
- Staff and governor training
- Behaviour policy
- Anti-Bullying policy
- Missing Pupil policy
- Use of Reasonable Force and Physical Restraint policy
- Hands On code of conduct
- Staff code of conduct
- Record of sanctions and disciplinary procedures
- Information on whom students can turn to if they are worried
- Departmental curricula, PSHE and sex education
- Learning Support and English as an Additional Language policies
- Alcohol, Smoking and Drugs policy
- Medical, First Aid and Self-Harm policies
- Healthy eating
- Health and safety including site and off site security
- Prefect training
- Gap student training
- School risk assessments
- Fire policy
- Supervision and registration procedures
- Admission and attendance registers
- Visitors to the school
- Educational visits
- Equal opportunities
- Parent communication
- Emergency procedures
- Use of photographs and film
- Appropriate posters giving contact numbers for child protection helplines
- Whistleblowing policy
- Complaints policy
- Staff Grievance and Disciplinary procedures
- Distance Learning agreement policy

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. Coming into our education system are digital natives, who have grown up with internet access. 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, as well as the social opportunities that these new technologies offer.

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
- Apps
- 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 including tablets and gaming devices
- Online Games
- Learning Platforms and Virtual Learning Environments
- Blogs and Wikis
- Podcasting
- Video sharing
- Downloading
- On demand TV and video, movies and radio / Smart TVs

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 (13 years in most cases).

Both this policy and the Acceptable Use Agreement (for all staff, governors, visitors and pupils) are inclusive of both fixed and mobile internet; technologies provided by the school (such as PCs, laptops, mobile devices, webcams, whiteboards, digital video equipment, Wi-Fi etc); and technologies owned by pupils and staff, but brought onto school premises (such as laptops, mobile phones and other mobile devices).

Roles and responsibilities

E-Safety Officer:

Named point of contact and takes day to day responsibility for E-safety issues.

Ensures that all staff are aware of the policies and procedures that need to be followed in the event of an E-safety incident taking place.

Provides training and advice for staff, students and parents.

Liaises with the DSP and with the school IT department.

Receives reports of E-safety incidents and creates a log of incidents to inform future E-safety developments.

Keeps up to date with E-safety technical information in order to effectively carry out their E-safety role and to inform and update others as relevant.

Director of IT:

Ensures that the school's ICT infrastructure is secure and is not open to misuse or malicious attack.

Ensures that users may only access the school's networks through a properly enforced password protection policy.

Ensures the school's filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person.

Keeps up to date with E-safety technical information in order to effectively support the E-safety role and to inform and update others as relevant.

Teaching and Support staff are responsible for ensuring that:

They have an up to date awareness of E-safety matters and of the current school E-safety policies and practices as well as the safeguarding risks attached to use.

They have read and understood the school Staff Acceptable Use Policy.

They report any suspected misuse or problem to the E-safety Officer / Director of IT / DSP for investigation / action / sanction.

Photographs and video clips are never taken, received or shared of a student that could compromise the student's dignity.

Digital communications with students are on a professional level and only carried out using official school systems.

E-safety issues are embedded in all aspects of the curriculum and other school activities.

Students understand and follow the school e-safety and Acceptable Use Policy.

Students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.

They monitor ICT activity in lessons, extracurricular and extended school activities.

They are aware of E-safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices.

They do not use personal digital devices to record school data, images or pupil information.

In lessons where internet use is pre-planned students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

Designated senior person for child protection:

Is trained in E-safety issues and is aware of the potential for serious child protection issues to arise from:

Sharing of personal data;

Access to illegal / inappropriate materials;

Inappropriate on-line contact with adults / strangers;

Potential or actual incidents of grooming;

Radicalisation;

Cyber-bullying; and

The Prevent duty.

Leadership and management team:

Develop an online safety culture throughout the school as part of safeguarding, which is in line with national best practice recommendations and the regulatory requirements for England.

Ensure that online safety is clearly identified and established as part of the roles and responsibility of the management/senior leadership team and governing body etc.

Audit and evaluate current practice to identify strengths and areas for improvement.

Embed online safety in staff training and professional development by ensuring that all members of staff receive up-to-date and appropriate online safety training (at least annually and as part of induction) and guidance which sets out clear boundaries for safe and professional online conduct online.

Students:

Are responsible for using the school ICT systems in accordance with the Student Acceptable Use Policy.

Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.

Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.

Will be expected to know and understand school policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand school policies on the taking / use of images and on cyber-bullying.

Should understand the importance of adopting good E-safety practice when using digital technologies out of school and realise that the school E-Safety Policy covers their actions out of school.

Parents / Guardians

Tring Park will take every opportunity to help parents understand E-safety issues through parents' evenings, letters home offering advice, E-safety talks and drop in sessions.

Monitoring, breaches and reporting

Monitoring

Authorised ICT staff may inspect any ICT equipment owned or leased by the school at any time without prior notice.

ICT authorised staff may monitor, intercept, access, inspect, record and disclose telephone calls, e-mails, instant messaging, internet/intranet use and any other electronic communications (data, voice, video or image) involving its employees or contractors, without consent or notice, 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 current data protection legislation, 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 current data protection legislation, 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.

For staff any policy breach is grounds for disciplinary action in accordance with the school Disciplinary Procedure.

Policy breaches may also lead to criminal or civil proceedings.

Incident reporting

Students must know to switch off the monitor or close the laptop if they find something unpleasant or frightening and then talk to a member of staff or the E-safety Officer.

Staff must report any E-safety incidents to the E-safety Officer, DSP or the Director of IT. Switch off the monitor or close the laptop, do not make any attempts to copy or save evidence, instead preserve it by isolating the device and reporting the situation. See appendix A for flowchart of incident reporting.

All security breaches, lost/stolen equipment or data, virus notifications, unsolicited emails, misuse or unauthorised use of ICT and all other policy non-compliance must be reported to the IT department.

Education & training - Students

E-safety education will be provided in the following ways:

A planned E-safety programme will be provided as part of ICT / PHSE / other lessons and should be regularly revisited – this will cover both the use of ICT and new technologies in school and outside school. The school brings in industry professionals to run age appropriate workshops, to enhance the delivery of the E-safety messages to the student body.

Key E-safety messages should be reinforced as part of a planned programme of assemblies and tutorials and drop in sessions in the pastoral areas.

Students / pupils should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.

Students should be helped to understand the need for the student AUP and encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school.

Students should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.

Staff should act as good role models in their use of ICT, the internet and mobile devices.

Education & Training – Staff

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

A planned programme of formal E-safety training will be made available to staff. An audit of the E-safety training needs of all staff will be carried out regularly.

All new staff should receive E-safety training as part of their induction programme, ensuring that they fully understand the school E-safety Policy and Acceptable Use Policy.

The E-Safety Officer (or other nominated person) will provide advice / guidance / training as required to individuals.

Inappropriate and illegal Online Activity, Actions and Sanctions

User Actions		Unacceptable	Unacceptable and Illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	child sexual abuse images		✓
	promotion or conduct of illegal acts, eg under the child protection, obscenity, computer misuse and fraud legislation		✓
	adult material that potentially breaches the Obscene Publications Act in the UK		✓
	criminally racist material in UK		✓
	pornography	✓	
	promotion of any kind of discrimination		✓
	promotion of racial or religious hatred		✓
	threatening behaviour, including promotion of physical violence or mental harm		✓
	any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute	✓	
Using school systems to run a private business		✓	
Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school		✓	
Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions			✓
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)			✓
Creating or propagating computer viruses or other harmful files			✓
Carrying out sustained or instantaneous high volume network traffic (downloading / uploading files) that causes network congestion and hinders others in their use of the internet		✓	

Prevent Extremism and Radicalisation

Since the Government's publication of the Prevent Duty Guidance, there has been an awareness of the specific need to safeguard children, young people and families from violent extremism. There have been several occasions in which extremist groups have attempted to radicalise vulnerable children and young people to hold extreme views including views justifying political, religious, sexist or racist violence, or to steer them into a rigid and narrow ideology that is intolerant of diversity and leaves them vulnerable to future radicalisation.

As a school we have regard for the Prevent Duty Guidance, and recognise that safeguarding against radicalisation is no different from safeguarding against any other vulnerability. All staff are expected to uphold and promote the fundamental principles of British values, including democracy, the rule of law, individual liberty and mutual respect, and tolerance of those with different faiths and beliefs.

Our curriculum promotes respect, tolerance, diversity and fundamental British values. Children are encouraged to share their views and recognise that they are entitled to have their own different beliefs which should not be used to influence others.

As part of wider safeguarding responsibilities school staff will be alert to:

- Be alert to changes in behaviour which could indicate that someone may be in need of help or protection (such as emotional changes, showing sympathy for extremist views, withdrawal, identity crisis, isolation or changes in physical appearance).
- Disclosures by students of their exposure to the extremist actions, views or material.
- Graffiti symbols, writing or art work promoting extremist messages or images.
- Students accessing extremist material online, including through social networking sites.
- Parental reports of change in behaviour, friendship or actions and requests for assistance.
- Students voicing opinions drawn from extremist ideologies and narratives.
- Use of extremist or 'hate' terms to exclude others or incite violence.
- Intolerance of difference, whether secular or religious or, in line with our equalities policy, views based on, but not exclusive to, gender, disability.
- Homophobia, or any form of discrimination based upon race, colour or culture.
- Anti-Western or Anti-British views.

Any indicators or incidents will be reported to the Designated Safeguarding Lead.

All incidents will be fully investigated and recorded.

Parents will be contacted and the incident discussed in detail, aiming to identify motivating factors, any changes in circumstances at home, parental views of the incident and to assess whether the incident is serious enough to warrant a further referral. A note of this meeting will be kept on the student's file.

In the event of a referral relating to serious concerns about potential radicalisation or extremism, the school will immediately contact the DfE helpline for radicalisation and extremism on 0207 7347264. This helpline is for non-emergencies. In an emergency, such as where a child is at immediate risk or there is a security incident, the Hertfordshire Police Prevent Team, MASH team,children's social services and/ or , CHANNEL will be contacted, as appropriate.

Peer on Peer Abuse

All staff should be aware that children can abuse other children (often referred to as peer on peer abuse). This can occur through the use of technology in the form of cyberbullying or upskirting. Upskirting typically involves taking a picture under a person's clothing without them knowing, with the intention of viewing their genitals or buttocks to obtain sexual gratification, or cause the victim humiliation, distress or alarm. It is a criminal offence. Further details can be found in the School's Anti-bullying policy and Safeguarding and Child Protection policy.

Use of digital and video images - Photographic, Video

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students instant use of images that they have recorded themselves or downloaded from the internet. However, staff and students need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet indefinitely and may cause harm or embarrassment to individuals. There are many reported incidents of employers carrying out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

When using digital images, staff should inform and 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, e.g. on social networking sites.

Staff are allowed to take digital / video images to support educational aims, which do not compromise the dignity of another student or staff member and must follow this policy concerning the sharing, distribution and publication of such images. Such images should only be taken on school equipment; the personal equipment of staff must never be used for such purposes.

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.

Students must not take, use, share, publish or distribute images of others without their permission.

Photographs of students published on the website, or elsewhere, will be selected carefully and will comply with good practice guidance on the use of such images.

ICT Equipment

All purchasing / procurement of ICT equipment / hardware must be done in conjunction with the Director of IT.

In some cases staff may be assigned equipment directly to them for their use in their role. Such staff are responsible for the care and safe-keeping of that equipment and must ensure that it remains in good working condition with no damage.

Any damage caused to the equipment assigned to a member of staff should be reported to the Director of IT & or their Line Manager at the first available opportunity.

Laptops or similar devices that have been provided to a member of staff should only be used by that person and only for carrying out their professional activities for Tring Park.

Staff laptops must be given to the IT department once a term for maintenance tasks. In most cases this may only take an hour or two but staff should allow for one working day.

When using any ICT equipment staff should act in a responsible manner ensuring that Health & Safety considerations are met at all times.

Any user of the ICT infrastructure network who is considered to be a 'Display Screen User' under the Health and Safety (Display Screen Equipment) Regulations 1992 (the "Regulations") will undergo a Health & Safety assessment in accordance with the Regulations. The Regulations set out ways to minimise the risks in using computers by ensuring that workplaces and jobs are well designed. See Staff Resources – Health & Safety for workstation checklist and self-assessment form for more details and contact the IT department if any assistance with the assessment is required or if there are any queries raised.

Staff and students must help protect the school's ICT systems by regularly applying the necessary updates and patches to personal equipment and having anti-virus and spyware protection that is regularly updated and the device scanned. This is particularly relevant when using personal pen drives / memory sticks on school systems or accessing remote services such as the school's MIS or email.

Software

Tring Park School strives to ensure that it remains legally compliant with Software Licensing.
In order for Tring Park to remain legally compliant the following must be adhered to:

- The purchase of new software must have been consulted with and approved by the Director of IT.
- Under no circumstances must personally owned software be installed or attempted to be installed on any Tring Park equipment (including memory sticks).
- Only authorised members of staff can install software. Please consult the Director of IT for any queries.
- Software must not be downloaded from the Internet and installed or attempted to be installed on any Tring Park equipment.
- It will be considered a disciplinary offence should any person use or attempt to use any piece of software on any Tring Park ICT equipment which knowingly has an adverse or detrimental effect on the ICT network or as a whole or which compromises the data on the systems.

Prohibited Software:

- Software intended to subvert the security of any computer system, or seek vulnerabilities.
- Software intended to compromise any user's password or system password.
- Software intended to intercept network traffic.
- Software which has been obtained illegally or in breach of any licence agreement.
- Peer to peer filesharing software or any applications that involve committing Tring Park to sharing its network bandwidth in an uncontrolled and unlimited way e.g. Kazaa, BitTorrent, DirectConnect.
- Applications that may introduce viruses or "spyware" when run.
- Download managers.
- HTTP tunnelling software.
- Share scanning software, such as Sharescan, LANster.

File management

All staff have access to four locations to store files:

- OneDrive Personal Folder (O:) – can only be accessed by the user and system administrators.
- Staff Resources – In progress migration from on-site storage to Teams file storage by department and an all staff team. Contact the IT department for any changes or to check folder access.
- Student Resource – A student Team's site - Folders can be set up to distribute work to the students. Confirm with the IT department if access needs to be restricted or content protected.
- Media Resources – On-site storage for large media files stored for teaching purposes.

All Students have access to two locations to store files:

- OneDrive Personal Folder (O:) – can only be accessed by the user and system administrators.
- Student resource – Team's site

All users are responsible for ensuring that the data stored in files and folders is appropriate and does not contain any explicit or implicit material, offensive comments about race, gender, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs, or national origin.

Users must not store any personal, non-school data on the Tring Park ICT network. Any data that is found to be non-school data will be deleted without question. Tring Park takes no responsibility for loss of or damage to any user's non-school data.

Users are also responsible for regular housekeeping of their Personal Folder and any shared folders that they have access to. File areas have a limited amount of storage space therefore any unwanted or unnecessary files should be deleted.

All storage areas containing files (personal & shared) are backed up. The IT department should be able to restore any data dependant on the backup retention. Please be aware that the local drives on computers are not backed up so saving data on the C: or desktop can be lost through hardware failure or maintenance tasks. The IT department are always available to help with any queries on how data is stored.

Email Usage

All members of staff are provided with access to an email address in the form of *firstname.lastname@tringpark.com*. The email facility is provided by the school to enable communication between staff and outside agencies in relation to Tring Park business.

This section sets out the proper use of email for Tring Park related purposes.

All staff must access their email at least twice each working day and must regularly perform housekeeping maintenance on all folders within their mailbox. It is suggested that users use a folder structure to store emails that they wish to keep and delete as soon as possible any un-needed and unnecessary emails.

Tring Park's email system is intended for the sole purpose of school business. It is agreed and understood that personal emails may be received and/or sent using a Tring Park email account, however this should be kept to a minimum and should not disrupt or distract the individual from the conduct of school business or cause the restriction of use of these systems to other legitimate users. The School reserves the right o access any email account on the Tring Park system and would be subject to searches for any Data Subject Access Requests (DSAR) received under the Data Protection Act.

All users must be vigilant when using their email address to "sign-up" to any Internet website, newsletter or other publication. Users must not use their email address in this manner for any personal use. It must be understood that this practice is a common area used by "Spammers" and therefore signing up to a website or newsletter can result in an increase in traffic of emails both to the user and to the Tring Park e-mail service.

Ensure that:

- You have applied the school disclaimer to your email account.
- You notify the sender of any email message which you receive in error.
- You take care before entering into contractual agreements by email.
- Only send emails to those who require the information.
- Do not send documents as attachments to staff when the document can or could be accessed on a shared area.
- Apply good email etiquette such as avoiding uppercase or red text that is considered aggressive.

When using the email system you must not:

- Send information that may breach Tring Park's policies or government regulations. This includes messages that may harass or offend (including racist, sexist information including defamation or obscenity).
- Distribute chain mail.
- Send messages from someone else's account except under proper "delegate" arrangements which retain individual accountability.

- “auto forward” mail to a unsupported system or other mail account, this includes internet and other public networks.
- Forward information known or believed to be confidential without the approval of the sender or information owner. If you are unsure whether the information is confidential, assume that it is.
- Use your Tring Park email address to sign up on Internet websites for personal use.
- Create email congestion by sending trivial messages or unnecessarily copying emails.

Internet filtering and monitoring

The school endeavours to do all it reasonably can to protect pupils from potentially harmful and inappropriate online material, without over blocking access to the internet, by using appropriate filtering and monitoring on school devices and the school network.

The school uses Smoothwall Filter and Firewall to manage internet access and protect the network. The internet filter is customised to apply different levels of filtering and protection to each pupil year group, and this allows the school to manage age related content by allowing or blocking different categories and web addresses. It also stops access at night giving different ‘lights out’ times for different pupil years.

The filter uses real time dynamic content analysis to categorise new and existing web content by analysing the content, context and construction of each page. The firewall is a unified threat management solution that protects the network with a perimeter firewall, packet inspection, intrusion detection and prevention.

Staff and pupils are encouraged to report any websites they believe are incorrectly blocked to the school for review by submitting a request to support@tringpark.com. Any website access that is flagged or blocked is reviewed, logged and passed on either to the e-safety officer or the DSL as appropriate.

This system is regularly updated and the list of blocked websites is constantly updated by the company providing the service. The Director of IT, DSL and the SLT also regularly review the school’s filtering and monitoring provision and effectiveness of its security protection procedures in order to safeguard its information security and data access management systems from cyber-crime technologies. The school is mindful of the DfE’s guidance ‘Meeting digital and technology standards in schools and colleges’ and ‘Cyber security standards for schools and colleges’.

Due to the scale of the challenge and students’ connectivity on personal devices at school and at home, the school believes the correct approach is through education alongside an appropriate level of filtering and monitoring. The filter is a tool to try and limit students’ access to inappropriate content but it is not as effective as equipping young people to protect themselves.

The internet filter settings are audited annually by the Director of IT, DSL and E-safety officer.

The internet usage logs are checked each week and any inappropriate activity is flagged and passed to the Director of IT. DSL and the E-safety officer as appropriate. This includes any sites that should be covered by the Prevent Duty Guidance. Instant alerts are emailed from the filtering system to the IT department, if required, any concerns can be addressed in real time before the weekly review.

Very occasionally a flagged URL may be checked by a member of the IT department or E-safety Officer to query against false positives. This usage will be recorded and monitored by the system as the IT department's internet access is monitored along with every member of staff.

Internet usage must not be used for the investigation, creation or distribution of any disruptive or offensive material. This includes, but is not limited to, explicit or implicit material that contains offensive comments about race, gender, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs, or national origin. This service may also not be knowingly used for any activity which is illegal under any legislation.

Data security

This part of the policy should be read in conjunction with the school's Data Protection Policy.

Tring Park's computing resources, data, information and information processes must be protected from unauthorised use, external intrusion and accidental or malicious damage. This section of the policy outlines measures put in place by the school to protect users and their data.

Staff that have ICT equipment assigned to them or borrow ICT equipment to take offsite must fully understand the protection of data and ensure that any data held on the equipment is fully protected as far as possible with any access controls, such as password protection.

All data must be processed in accordance with the school's Data Protection Policy – Privacy Standard and current data protection legislation.

An unattended computer/laptop may provide an opportunity for unauthorised access to computing resources, information and user data.

Staff using ICT equipment must ensure that they adhere to the following:

- Close down active sessions and log out of, or lock the workstation using the Ctrl+Alt+Delete buttons if the computer/laptop is being left unattended.
- Log out at the end of each day, do not leave the computer locked, as any open files may not be backed up.
- Do not store sensitive information on any area of the ICT network that is unrestricted or on any local drive.

A password policy is enforced so passwords must be over six characters in length and not match any of the previous ten. All staff have to use complex passwords and 2fa to access Microsoft 365 and the School Management Information system ISAMS.

All school computers are remotely managed and protected by an anti-virus system. Microsoft SCCM applies Microsoft updates to onsite devices and Intune updates remote/mobile staff devices.

Remote working

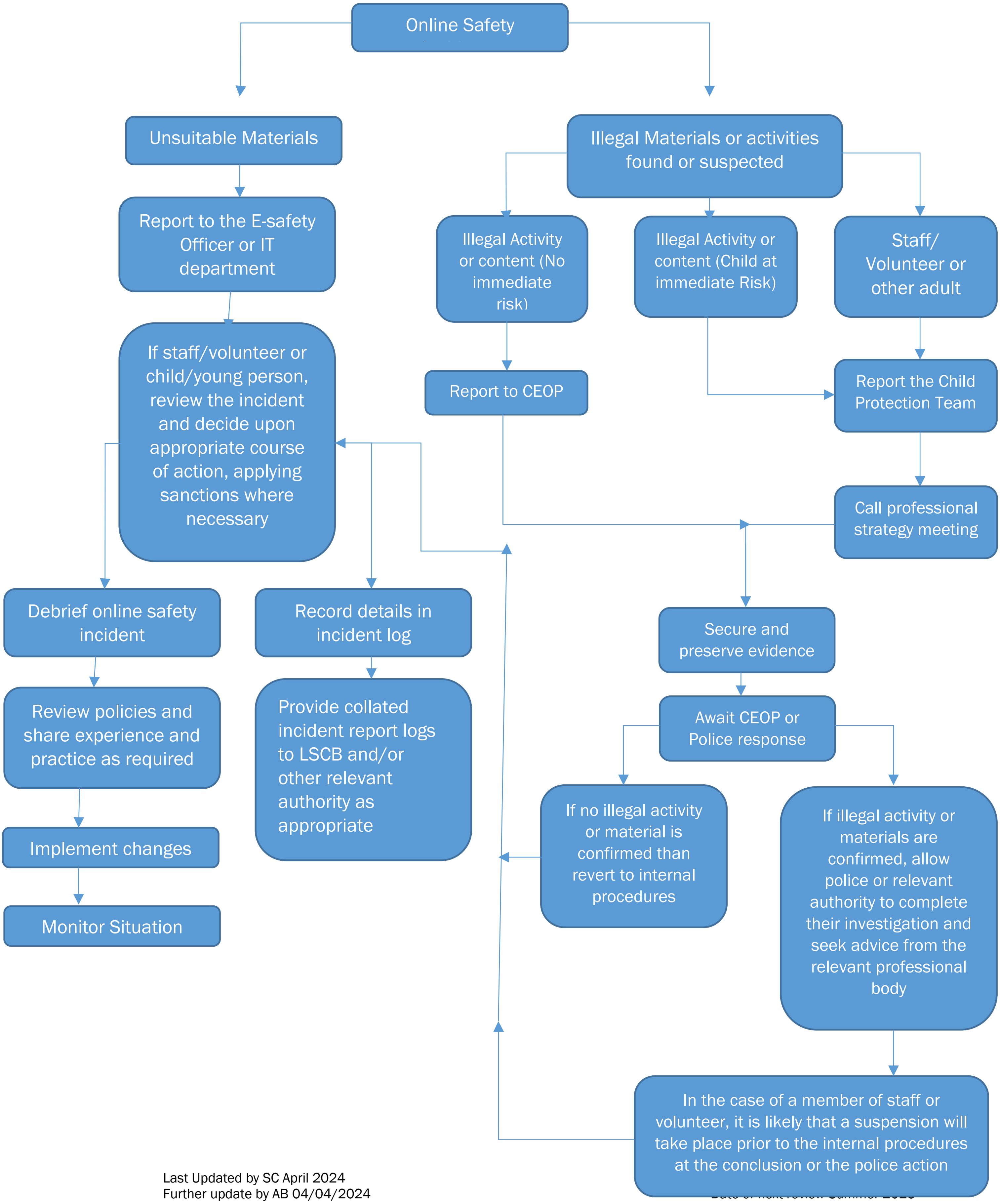
- When working or accessing school systems remotely, safeguarding pupils and data privacy best practice must be applied.
- If using personal devices to access school systems, apply available updates and security patches.
- Update and scan with anti-virus software.

- Apply screen locks to mobile devices.
- Don’t leave connections to school systems such as email, files, ISAMS or Teams unattended.
- The distance learning agreement (Appendix G) sets out how teachers and pupils will agree to use the systems in place for distance learning.

Distance learning agreement

The school has its distance learning agreement on file in case of any future need for online/remote teaching as in the event of another lockdown.

Appendix A - E-safety incident flowchart


Online Safety
Unsuitable Materials
Illegal Materials or activities found or suspected
Report to the E-safety Officer or IT department
Illegal Activity or content (No immediate risk)
Illegal Activity or content (Child at immediate Risk)
Staff/ Volunteer or other adult
If staff/volunteer or child/young person, review the incident and decide upon appropriate course of action, applying sanctions where necessary
Report to CEOP
Report the Child Protection Team
Call professional strategy meeting
Debrief online safety incident
Record details in incident log
Secure and preserve evidence
Review policies and share experience and practice as required
Provide collated incident report logs to LSCB and/or other relevant authority as appropriate
Await CEOP or Police response
Implement changes
If no illegal activity or material is confirmed than revert to internal procedures
If illegal activity or materials are confirmed, allow police or relevant authority to complete their investigation and seek advice from the relevant professional body
Monitor Situation
In the case of a member of staff or volunteer, it is likely that a suspension will take place prior to the internal procedures at the conclusion or the police action

Last Updated by SC April 2024
Further update by AB 04/04/2024

Appendix B – Staff and Governor Acceptable Use Agreement

IT Acceptable Use Policy Agreement for Staff & Governors

Acceptable Use Policy Agreement

I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users. I recognise the value of the use of ICT for enhancing learning and will ensure that students receive opportunities from the use of ICT. I will, where possible, educate the students in my care in the safe use of ICT and embed E-safety in my work with students.

For my professional and personal safety:

- I understand that the school will monitor my use of the ICT systems, email and other digital communications.
- I understand that the rules set out in this agreement also apply to use of school ICT systems e.g. laptops, email, ISAMS, etc.) outside of school.
- I understand that the school ICT systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set out by the school.
- I will not disclose my username or password to anyone else, nor will I try to use any other person’s username and password.
- I will immediately report any illegal, inappropriate or harmful material or incident I become aware of to the appropriate person.
- I will be professional in my communications and actions when using school ICT systems
- I will not access, copy, remove or otherwise alter any other user’s files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will only use chat and social networking sites in school in accordance with the school’s policies.

- I will only communicate with students and parents / carers using official school systems. Any such communication will be professional in tone and manner. Any communication with former pupils will continue to be professional in tone and manner.

- I will not engage in any on-line activity that may compromise my professional responsibilities.

- I understand that the school has responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- When I use my personal hand held / external devices (PDAs / laptops / mobile phones / USB devices etc.) in school, I will follow the rules set out in this agreement and in the mobile phone policy in the same way as if I were using school equipment. I will also follow any additional rules set by the school about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.

- I will not open any attachments to emails, unless the source is known and trusted, owing to the risk of the attachment containing viruses or other harmful programmes.

- I will not try to upload, download or access any materials which are illegal (e.g. child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.

- I will not try, unless I have permission, to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.

- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless I confirm first with the Director of IT.

- I will not disable or cause any damage to school equipment, or the equipment belonging to others.

- I understand that the school's Data Protection Policy – Privacy Standard requires that any staff or student data to which I have access will be kept private and confidential, except when I am required by law or by school policy to disclose such information to an appropriate authority.

- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the internet in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work.

- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

I am responsible for my actions in and out of school and confirm that:

- I understand that this Acceptable Use Agreement applies not only to my work and use of school ICT equipment in school, but also applies to my use of school ICT systems and equipment out of school and my use of personal equipment in school or in situations related to my employment by the school.

- I understand that if I fail to comply with this Acceptable Use Agreement, I could be subject to disciplinary action up to and including termination of employment. This could include a warning, a suspension, a referral to Governors and, in the event of illegal activities, the involvement of the police.

Appendix C - Student Acceptable Use Agreement

IT Acceptable Use Agreement for Pupils

I understand that I must use the school ICT systems in a responsible way to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users.

For my own personal safety:

- I understand that the school will monitor my use of the ICT systems, email and other digital communications.
- I will not share my username or password with anyone, nor will I try to use any other person's username or password.
- I will be aware of "stranger danger", when I am communicating on-line.
- I will not disclose or share personal information about myself or others when on-line.
- If I arrange to meet people off-line whom I have communicated with on-line, I will do so in a public place and take an adult with me.
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.

I understand that everyone has equal rights to use technology as a resource and:

- I understand that the school ICT systems are primarily intended for educational use.
- I will not try, unless I have permission, to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not use the school ICT systems for on-line gaming, on-line gambling, internet shopping, file sharing, or video broadcasting (e.g. YouTube), unless I have permission from a member of staff to do so.
- I will treat School computers and peripheral equipment with respect at all times. I will act as I expect others to act toward me.
- I will only use the printing system for educational use and will not waste paper and toner.
- I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.
- I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will not take or distribute images of anyone without their permission.

I recognise that the school has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the smooth running of the school, therefore:

- I will only use my personal hand held / external devices (mobile phones / USB devices etc.) in school if I have permission and in accordance with the school's mobile phone policy. I understand that, if I do use my own devices in school, I will follow the rules set out in this agreement, in the same way as if I were using school equipment.
- I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I will not open any attachments to emails, unless I know and trust the person / organisation that sent the email, because of the risk of the attachment containing viruses or other harmful programmes.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings.
- I will not use or bring into school any key loggers or similar devices that capture activity on a device.
- I will only use chat and social networking sites with permission or at the times that are allowed.
- I understand personal laptop computers will be subject to scrutiny to ensure that no inappropriate material is held.

When using the internet for research or recreation, I recognise that:

- I should ensure that I have permission to use the original work of others in my own work.
- Where work is protected by copyright, I will not try to download copies (including music and videos).
- When I am using the internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.

I understand that I am responsible for my actions, both in and out of school and:

- I understand that the school also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve my membership of the school community (examples would be cyber-bullying, use of images or personal information).
- I understand that if I fail to comply with this Acceptable Use Agreement, I will be subject to disciplinary action. This may include loss of access to the school network / internet and, in the event of illegal activities, involvement of the police. Persistent and serious abuse will be considered as a major disciplinary issue and may lead to suspension and/or expulsion.

The school reserves the right, without further notice or permission, to inspect your device and access data and applications on it, and remotely review, copy, disclose or wipe, enabling us to: inspect the device for use of unauthorised applications or software; investigate or resolve any security incident or unauthorised use of school systems; ensure compliance with our rules, standards of conduct and policies in force from time to time (including this policy). You must co-operate with the school to enable such inspection, access and review, including providing any

passwords or pin numbers necessary to access the device or relevant applications. A failure to co-operate with the school in this way may result in sanctions, up to and including expulsion.
If the school discovers or reasonably suspects that there has been a breach of this policy, including any of the security requirements listed above, your access to school systems will be immediately removed.
By signing the declaration at the end of this policy, you consent to the school, without further notice or permission, inspecting a device and applications used on it, and remotely reviewing, copying, disclosing, wiping or otherwise using data on or from a device that is in breach of this policy.

Appendix D – Online safety information

Guidance on how to be safe in the digital environment

Mobile phone safety

The rules set out in the school's mobile phone policy are there to keep all pupils and the community safe which is why it is important that everyone adheres to it.
Keep your phone with you at all times. If you are worried about someone taking it at school or when are out, leave it at home or with a houseparent.
Only give your mobile number to your friends and people whom you trust.
Don't lend your phone to someone you don't know or trust, or put it in a place where other people could get hold of it.
Most phones allow you to lock your phone with a PIN code. Use your PIN to prevent anyone else from accessing tis content.
If someone is pressuring you into giving them your number, tell someone such as a teacher or a parent.

Staying Safe on Social Networking Sites

Use password protection at all times.
Only allow friends to see the content you post.
Protect your password and don't give it to anyone.
Make sure you really know who someone is before allowing them onto your friends list. Don't add anyone you don't know, even if they say they know you.
Don't post any photos or videos that you wouldn't be happy for your parents or teacher to see. Once photos are online they can be copied and posted to other places where you can't remove them.
Don't do or say anything online you wouldn't say offline.
Protect your privacy and your friends' privacy too: get their permission before posting anything about them.

How do I create a safe profile?

When you're online, you won't always know who you're chatting to. Most social networking sites allow you to change the security settings on your profile so it can only be seen by those you allow. They also let you choose who your friends are. Never use your real name or tell

anyone anything personal about yourself or your family such as your address, phone number, or school.
Instead of using a photo of you for your online profile picture, use a picture of something you like.
If someone contacts you or one of your friends with weird or nasty messages, don't reply to them but do save the messages. Tell someone you trust such as a parent or teacher as soon as possible and show them the message.
If you are writing a blog, be careful not to reveal too many personal details.
Don't arrange to meet someone whom you have met online as they may not be who they say they are. If you do decide to meet them, tell someone you trust such as a parent or teacher that you want to do this. Arrange to meet in a public place and take a trusted adult with you.

If you are contacted by someone you are unsure of on a forum, inform the forum administrator.

Avoid sites that are meant for adults.
If you are worried about anything to do with staying safe online, talk to your parents or a member of staff.

Appendix E – Visitor Acceptable Use Policy

Your usage of the guest Wi-Fi network constitutes your acceptance of this policy.

Use of the Internet via the guest Wi-Fi network and your own electronic device is subject to the same conditions as set out in the appropriate pupil or staff ICT Acceptable Use Agreement. You must ensure that your Internet usage whilst connected to the guest Wi-Fi network is in line with the Acceptable Use Agreements and appropriate within the school context.

As you are sharing the internet connection with students and staff please refrain from:

- Peer-to-peer file sharing (including, but not limited to the use of torrents).
- Use of any form of video/camera/audio facility on your electronic device to capture, record or stream at any time.
- Video and audio streaming of a non-educational nature (for example, using a website to catch up on TV).
- Using any form of 'proxy bypass' to bypass, or attempt to bypass, the School's Internet filtering system.
- Attempting to 'hack' or otherwise compromise the security and integrity of the guest Wi-Fi network.
- The use of 'tethering' or any other method to turn your electronic device into a Wi-Fi hotspot.
- In the interests of network performance, the School may restrict the data bandwidth and user experience to an individual user and electronic device, if it deems necessary.

This is a public Wi-Fi network and as such should be subject to the same precautions as any other public network. We advise you to ensure that your electronic device has suitable anti-virus and firewall security software installed, and that you set the network profile as 'public' or similar on your electronic device / firewall security software.

Guest Wi-Fi network and Internet activity is logged and monitored at all times, in order for us to meet with our E-safety and Child Protection responsibilities.

- Your access to the guest W-Fi network will be withdrawn with immediate effect if you fail to adhere to this Acceptable Use Agreement, or any other applicable school policy or guideline.
- Access to the guest Wi-Fi network may be restricted or withdrawn at any time, without notice, to ensure that the integrity and security of the network and/or other users are not compromised.

Connecting your electronic device to the school network is entirely at your own risk. The school will not be liable for any (hardware or software) loss, damage, malfunctioning or inconvenience to your electronic device arising either directly or indirectly as a result of its connection to the guest Wi-Fi network. It is your own responsibility to ensure that any software installed on your electronic device is correctly licensed.

Appendix G

Legal framework

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 and the UK GDPR

This protects the rights and privacy of individual's data. To comply with the law, information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully. The Regulations state that personal data must be:

- Processed fairly and lawfully and in a transparent manner.
- Collected for specified, explicit and legitimate purposes.
- Adequate, relevant and not excessive.
- Accurate and kept up-to-date.
- Not kept longer than necessary.
- Processed in accordance with the data subject's rights.
- Secure.
- Not transferred to other countries without adequate protection.

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 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.

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

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. (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 Head teachers, 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.