Document Title	**Online Safety Policy**
Committee Responsible for Policy	**Board of Directors (in consultation with Student Committees).**
Review Frequency	**Annually**
Last Reviewed	**October 2025**
Next Review Due	**October 2026**
Policy Author	**Associate Headteacher (Phil Bennett) and Director of Technical Services (Brian Kelly)**

Online Safety Policy

Contents

1 Introduction

ICT in the 21st Century is 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
- Learning Platforms and Virtual Learning Environments
- Email and Instant Messaging
- Chat Rooms and Social Networking
- Blogs and Wikis
- Podcasting
- Video Broadcasting
- Music Downloading
- Gaming
- Mobile/ Smart phones with text, video and/ or web functionality
- Other mobile devices with web functionality

The breadth of issues classified within online safety is considerable, but can be categorised into four areas of risk:

- **content:** being exposed to illegal, inappropriate, or harmful content, for example: pornography, racism, misogyny, self-harm, suicide, antisemitism, radicalisation, extremism, misinformation, disinformation (including fake news) and conspiracy theories.
- **contact:** being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.
- **conduct:** online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying, and
- **commerce:** risks such as online gambling, inappropriate advertising, phishing and or financial scams. If you feel your pupils, students or staff are at risk, please report it to the Anti-Phishing Working Group (https://apwg.org/).

(Keeping Children Safe in Education, 2025)

The Ofsted report into sexual harassment and abuse (2021) also reinforces these key areas of risk, especially in child-on-child sexual abuse and harassment that can occur online.

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.

At Twyford C of E Academies Trust we understand the responsibility to educate our students in Online 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.

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 phones/PDAs, tablets, webcams, interactive whiteboards/panels, remote learning platforms, voting systems, digital video equipment, etc.), and technologies owned by students and staff, but brought onto school premises (such as laptops, mobile phones, camera phones, PDAs and portable media players, etc.).

2 Roles and Responsibilities

As Online Safety is an important aspect of strategic leadership within each school, the Executive group and Directors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. An Online Safety team at each school consists of the Associate Headteacher, the safeguarding governor, the designated safeguarding lead, and the Director of Technical Services. It is the role of the Online Safety team to keep abreast of current issues and guidance through organisations such as Ealing LA, CEOP (Child Exploitation and Online Protection), Prevent strategy and Childnet. Improvements and actions are agreed at least annually between the team.

Senior Management and Governors are updated by the Online Safety team 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, supported by the school's Acceptable Use Agreements for staff, governors, visitors and students (appendices), 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.

2.1 Online Safety skills development for staff

- Our staff receive information and training on new Online Safety issues in the form of presentations to staff and governors and specific training modules
- New staff receive information on the school's acceptable use policy as part of their induction.
- All staff are made aware of individual responsibilities relating to the safeguarding of children within the context of Online Safety and know what to do in the event of misuse of technology by any member of the school community.

- All ICT teachers are encouraged to incorporate Online Safety activities and awareness within their curriculum.
- All staff have completed training in latest government guidance including risks posed to pupils online.

2.2 Managing the school Online Safety messages

- We endeavour to embed Online Safety messages across the curriculum whenever the internet and/or related technologies are used.
- The Online Safety Policy (in the form of the Home School Agreement) will be introduced to the students at the start of each school year.
- Online Safety posters will be prominently displayed.
- Restrictions are in place as administered by IT Services to promote Online Safety and security.

3 Online Safety in the Curriculum

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

- The Trust has a planned strategy for teaching internet skills in ICT lessons which can be found in the ICT curriculum.
- The Trust provides opportunities within ICT, RE and the PSHE workshop curriculum to teach about Online Safety and the issue is regularly revisited in an age-appropriate way throughout students' time in Trust schools.
- Our PSHE workshops have been updated in light of the Ofsted report into sexual harassment and abuse, as well as latest government guidance to support the pupils to stay safe from sexual harassment or child-on-child abuse.
- The PSHE workshop coverage in school ensures pupils are aware of the risks posed by the '4Cs' – content, contact, conduct and commerce
- Educating students on the dangers of technologies that maybe encountered outside school is also done informally when opportunities arise and as well as part of the Online Safety curriculum.
- Students are made 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 and respecting other people's information, images, etc. through discussion, modelling and activities.
- Students are made aware of the impact of online bullying ('cyberbullying'), 'sexting', radicalisation and other online dangers and how to seek help if they are affected by these issues. 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 Childline/CEOP report abuse button.

- Students are educated about the risks of content they face, in particular in regard to radicalisation in line with our Prevent Duty.
- Students are supported to recognise the risks posed by contact with people who they do not know online, and the potential links to exploitation and abuse that these might involve.
- Students also receive extensive support with their own online behaviour, especially with regard to the generation or sharing of explicit content.
- Students are taught to critically evaluate materials and learn good searching skills through cross curricular teacher models, discussions and via the ICT curriculum.

4 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 secret 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 Online Safety Policy.
- Staff receive cyber-security training which includes training on password security.
- Users are provided with an individual network, email and Learning Platform log-in username. From Year 7 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 others.
- If you think your password may have been compromised or someone else has become aware of your password report this to IT Services.
- Staff are aware of their individual responsibilities to protect the security and confidentiality of 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 Learning Platform/Managed Learning Environment to the browser/cache options (shared or private computer)
- In Trust schools, all ICT password policies are the responsibility of IT Services and all staff and students are expected to comply with the policies at all times.

5 Data Security

The accessing and appropriate use of school data is something that the school takes very seriously.

- Staff are aware of their responsibility when accessing school data. Level of access is determined by the Associate Headteacher
- Sensitive data can only be taken off the school premises if it is encrypted (See Data Protection and Confidentiality Policy).
- Systems are in place to ensure school data is only accessible with appropriate authorisation and is secured against data loss with appropriate backup arrangements (see the Business Continuity Plan).
- All staff have undertaken data protection training as part of their baseline training and induction package.

6 Managing the Internet safely

The internet is an open communication medium, available to all, 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 London Grid for Learning (LGfL) is logged and the logs are randomly but regularly monitored. Whenever any inappropriate use is detected it will be followed up.

- The Trust maintains students will have supervised access to Internet resources through the school's fixed and mobile internet technology.
- 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
- All users must observe software copyright at all times. It is illegal to copy or distribute school software or illegal software from other sources.

6.1 Control, filtering and monitoring

- School internet access is controlled through the LGfL's web **filtering** service
- In addition, the Trust also manages some bespoke web filtering which is the responsibility of IT Services
- The Trust is aware of its responsibility when monitoring staff communication under current legislation and takes into account: General Data Protection Regulation 2016, 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 Trust does not allow students access to internet logs
- The Trust 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 IT Services or Director of Technical Services
- Anti-Virus protection is set to automatically update on all school machines and staff laptops. This is the responsibility of IT Services
- Staff are not permitted to download programs or files on school based technologies without seeking prior permission from the Director of Technical Services
- Students are not permitted to download or install programs
- If there are any issues related to viruses or anti-virus software, IT Services should be informed via the helpdesk.

7 Managing other Web 2 technologies

Web 2, 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 Trust denies access to social networking sites to students within school
- The schools do not permit smartphones in school in Key Stage 3 and 4 and on all school trips, to safeguard students from negative impacts on learning, but also to minimise the chances of inappropriate content being shared between students
- All students are advised to be cautious about the information given by others on sites, for example users not being who they say they are
- Students are encouraged to avoid placing images of themselves on such sites 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 such sites which may identify them or others
- Students are advised to set and maintain profiles on such sites to maximum privacy and deny access to unknown individuals
- Students are encouraged to be wary about publishing specific and detailed private thoughts online
- Our students are asked to report any incidents of bullying to the school
- Staff understand that it is forbidden to use open social networking sites - Facebook, WhatsApp, Instagram, etc. and public chat room facilities with students. They are expected to use the tools within the VLE as they become available.

8 Artificial Intelligence technologies

Artificial Intelligence (AI) applications incorporate machine learning that performs actions based on knowledge 'learned' from a database of example information. Systems are becoming available that perform tasks that are complex or time consuming for human operators, such as recommending websites or information, making decisions and creating written or artistic content ('Generative AI'). AI has potential to benefit our staff and students but also comes with risks. The Trust has adopted a separate AI Policy which includes safeguards to reduce the risk of adverse results or data protection breaches from the use of AI systems.

9 Mobile technologies

Many emerging technologies offer new opportunities for teaching and learning. Many existing mobile technologies such as portable media players, PDAs, gaming devices, mobile and Smart phones are 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 Trust chooses to manage the use of these devices in the following ways so that users exploit them appropriately.

9.1 Personal Mobile devices including phones

- The Trust allows staff to bring in personal mobile phones and devices for their own use. Under no circumstances does the Trust allow a member of staff to contact a student using their personal device.
- Student mobile phones (in years 7-11) are not permitted in school except the basic devices specified in the Behaviour Policy.
- The Trust is not responsible for the loss, damage or theft of any personal mobile device
- Capturing images and video is not allowed by students/staff unless on Trust equipment and for educational purposes. Prior permission must be obtained before this capture can take place
- Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device
- Staff should only charge mobile phones from computer/laptop USB ports not chargers that plug into the wall due to the fire risk.

9.2 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 for offsite visits and trips, only these devices should be used

10 Managing e-mail

The use of email within most schools is an essential means of communication for both staff and students. In the context of school, email should not be considered private. We recognise that students need to understand how to style an email in relation to their age and good ‘netiquette’ for example in order to achieve ICT level 4 or above, students must have experienced sending and receiving emails.

- The Trust gives all staff their own school email account to use for all Trust business
- It is the responsibility of each account holder to keep their password secure. For the safety and security of users and recipients, all mail is filtered and logged; if necessary email histories can be traced. This 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 email addresses
- The Trust requires a standard disclaimer to be attached to all email correspondence, stating that, ‘the views expressed are not necessarily those of the Trust’
- E-mail sent to an external organisation should be written carefully before sending, in the same way as a letter written on school or Trust headed paper
- All e-mail users are expected to adhere to the generally accepted rules of network etiquette (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.
- All attachments are automatically checked for viruses.
- Students must immediately tell a teacher/trusted adult if they receive an offensive message and keep the offending message(s) as evidence.
- Staff must inform the helpdesk if they receive an offensive e-mail.
- Students are provided with email accounts and are introduced to email as part of the ICT Scheme of Work.

11 Safe Use of Images / Film

11.1 Taking of Images and Film

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

- With the documented consent of parents and staff (written or electronic), 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.

11.2 Consent of adults who work at the school

- Parents must seek permission to take photos/film school events, and must agree to NOT post photos on the Internet.

11.3 Publishing student's images and work

- On a child's entry to the school, all parents/guardians will be asked to give permission to use their child's work/photos
- Parents/ carers 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 designated staff have authority to upload to the public website or VLE.

11.4 Storage of Images

- Images/films of students are stored on the Trust's network.
- Rights of access to this material are restricted to the teaching staff and students within the confines of the Trust network/VLE.

11.5 Webcams and CCTV

- The Trust uses CCTV for security and safety. The only people with access to this are Facilities management, SLT, IT Services
- Notification of CCTV use is displayed at the front of each school.

12 Remote Teaching and Learning

During times when it is not possible for a teacher or students to attend school it may be necessary for classes to be taught remotely, using the Microsoft Teams platform or similar. This is a great tool for enabling learning to continue but like most technology it comes with risks. This section of the policy details those risks and how the Trust will mitigate them.

12.1 Set up and Use of the Remote Learning Platform

Trust schools use the Microsoft Teams platform for remote learning. Other platforms are not currently approved for use for remote learning within Trust Schools. The Director of Technical Services is responsible for ensuring that Teams is set up to minimise the risk of inappropriate use. It is Trust policy to disable video for pupils attending remote lessons. Breakout rooms are not used. Students must be admitted to the lesson by the teacher to reduce the risk of a person entering an online lesson who is not a member of the school community. Online lessons are not recorded.

12.2 Teaching a Remote Lesson

If teaching from home, teachers are expected to ensure the background of their video is blank or filtered and there is no background noise. Teachers monitor attendance at remote lessons to ensure safeguarding expectations are met and they record the pupils' attendance on SIMS as if the pupil were attending an ‘in-person’ lesson. Staff would maintain appropriate and professional boundaries at all times in line with what is expected in a classroom setting.

12.3 Etiquette for Participants in Remote Lessons

Pupils in remote lessons are required to mute their microphone when they are not asked to speak. Pupils must not record remote lessons using software or devices or other means. Pupils must not allow others who are not part of the class to access or take part in lessons. Breaches of the expected Etiquette for participation in remote lessons is taken seriously and would be treated as a breach of the home-school agreement, acceptable ICT use agreement and the Trust’s behaviour policy.

12.4 Use of School Provided Devices

Where pupils have barriers to their engagement with online learning, third parties have issued schools with devices to issue to students to support them with their access to learning. Depending on the third-party, funding terms and conditions make clear if these devices are to become the property of the student or if they are school property which is being loaned to a pupil. Pupils and parents who receive these devices are notified if the device is their property which they can keep or school property which they should return at a specified time. The ICT team in conjunction with the pastoral team retains a log of which pupils are in possession of school devices. The pastoral team (Heads of Year and Heads of Key Stage) triage the levels of pupil need in order to distribute devices to pupils where third parties makes these available.

13 Misuse and Infringements

13.1 Concerns and Complaints

Concerns relating to Online Safety should be made to the Associate Headteacher in the first instance. The Trust Complaints Policy is available for formal complaints. All reported concerns or breaches of this policy are logged.

13.2 Inappropriate activity and material

- Inappropriate material includes (but is not limited to) content which is pornographic, discriminatory, or otherwise illegal or offensive.
- Inappropriate activity includes (but is not limited to) cyberbullying, grooming, ‘sexting’, hacking/activity which threatens the security of data and or systems.
- Accidental access to inappropriate materials must be reported to the IT Helpdesk.
- Deliberate access to inappropriate materials by students may lead to action being taken in accordance with the Behaviour Policy and, if illegal, to Police involvement.
- Deliberate access to inappropriate materials by staff may lead to action being taken in accordance with the Disciplinary Policy and, if illegal, to Police involvement.

14 Equal Opportunities

14.1 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 Trust's Online Safety rules.

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

15 Parental Involvement

We believe that it is essential for parents/carers to be fully involved with promoting Online Safety both in and outside of school. We regularly consult and discuss Online Safety with parents/carers and seek to promote a wide understanding of the benefits related to ICT and associated risks.

- Parents/carers and students are actively encouraged to contribute to adjustments or reviews of the Trust's Online Safety policy by the policy being discussed during PTFA meetings
- Parents/carers are asked to read through and sign acceptable use agreements on behalf of their child on admission to school (Appendix A).
- Parents/carers are required to make a decision as to whether they consent to images of their child being taken/ used in the public domain
- Each school disseminates information to parents relating to Online Safety where appropriate in the form of:
    - Information evenings
    - Posters
    - Website/ Learning Platform postings
    - Newsletter items

16 Writing and Reviewing this Policy

16.1 Staff and student involvement in policy creation

Where appropriate staff and students are consulted about the content of this policy through Union consultation and school council meetings.

16.2 Review Procedure

This policy will be reviewed every year and consideration given to the implications for future development planning. Changes may be required due to the adoption of new technologies or legal or regulatory changes.

Appendix A: Student Computer Use Agreement

COMPUTER USE AGREEMENT

The computer network at Twyford C of E Academies Trust is made available to students for the purposes of learning and educational research. Students are expected to behave responsibly in using the facilities and the purpose of this contract is to set out the rules for appropriate use. This agreement will enable students to use the ICT facilities for educational benefits. Please read it carefully, sign and return it to the School's Administration Department in order to access the school's network and Internet.

- I will comply with school rules for using computers (including the Online Safety Policy).
- I will only access the network via my own authorised account, which I understand is my own responsibility and I will not make available to anyone else except I may share login details with parents so they can access Copia.
- I will use the Internet appropriately for education purposes and will not attempt to access inappropriate web sites including sites that are pornographic, discriminatory, illegal or offensive.
- I understand that I am responsible for rejecting any unsuitable material and will report this to a member of staff.
- I understand that activity that threatens the integrity of the school ICT systems, or that attacks or corrupts other systems is forbidden.
- I will not do anything that might cause a breach of copyright, including downloading software, games, music, graphics, videos or text materials that are copyrighted.
- I will not use the network in any way that could bring the school's name into disrepute.
- I understand that the school network administrators have full access to the system and my account and that they reserve the right to examine or delete inappropriate files. I am also aware that my steps in using the network can be traced (including web sites visited).
- I understand that my parents may be required to meet the cost of replacing any school IT equipment which I damage.
- I will keep usernames and passwords for third party websites secret, and not allow anyone else access using my account
- I will abide by the rules of any third party websites that are used in school
- I will abide by the expected behaviour etiquette during online/remote lessons if for any reason I am learning at home via Microsoft Teams or other home-learning platform.

Acceptable Use Policy for Student Email

Use of email by students of Twyford C of E Academies Trust is permitted and encouraged where such use supports the goals and objectives of the school. All students are provided with their own email account for educational use only. Twyford C of E Academies Trust has a policy for the use of email whereby the students must ensure that they:

- Use email in an acceptable way
- Do not create unnecessary risk to the school by their misuse of the email system
- Comply with current legislation

Policy

- Students are responsible for the content of all emails sent.
- The sending of offensive, profane or abusive email or other messages is forbidden.
- If students receive any offensive or inappropriate emails they should report it to a teacher or the IT Services immediately.
- Use of school email accounts for bullying or harassment will not be tolerated as this is against school rules.
- Email attachments should only be opened if they come from a known and trusted source.
- The sending of email attachments containing any program, file or shortcut that damages or shuts down a computer, damages or alters the operating system or alters, deletes or otherwise modifies user files is strictly forbidden and is a criminal offence (Computer Misuse Act 1990).
- The use of email rules that disrupt, slow down or damage the email server or network system is not permitted.

Monitoring

Twyford C of E Academies Trust accepts that use of email is a valuable school tool. However, misuse of this facility can have a negative impact upon student productivity and the reputation of the school.

In addition, all of the school’s email resources are provided for school purposes. Therefore, the school maintains the right to examine any systems and inspect any data recorded in those systems.

Sanctions

If a student is found to have breached this agreement, they will face sanctions as set out in the Trust’s Behaviour Policy and withdrawal of access to the network and/or email service. Serious offences may result in temporary fixed term or permanent exclusion from school.

I understand that if I do not comply with this agreement I may face sanctions as outlined above I understand that each case will be considered on its merits.

Student name: ______________________________ Form: __________________

Student signature: ___________________________ Date: ___________________

Although the school makes every effort to ensure that students cannot access inappropriate material (through a filtering service and staff supervision), the nature of the Internet is such that there is no guarantee that ALL offensive sites have been blocked. However, the school believes that the benefits of providing access to ICT and the Internet far exceed the potential drawbacks and we hope that students will act responsibly in using the facilities they have been provided with.

I am aware that my child has been given access to the school's computer network and Internet and I have reinforced this agreement.

Parent/Carer signature: ______________________ Date: __________________

Appendix B: Staff Acceptable Use Agreement / Code of Conduct

This policy 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 Director of Technical Services.

- I will comply with Trust Policies concerning the use of ICT including the Online Safety Policy.
- I will only use the school's email / Internet / Intranet / VLE and any related technologies for professional purposes or for uses deemed 'reasonable' and appropriate 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, and never via personal email / phone.
- I will make professional use of online meeting platforms, such as Microsoft Teams, to support meetings with colleagues in school or other schools.
- I understand that messages I send on Trust systems – including email, Teams chat and voicemail – are not private. I will only communicate personal information or opinions about others which I would be happy to be disclosed to them.
- I will not give out my own personal details, such as mobile phone number and personal email address, to students.
- I will only use the approved, secure email system and VLE tools for communications with students and parents.
- I am aware that communicating with students via private email, SMS and social networking sites may be considered a disciplinary matter.
- I will ensure that personal data (such as data held on SIMS) 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.
- I will not install any hardware of software without permission of the Director of Technical Services.
- I will not browse, download, upload or distribute any inappropriate material including material that could be considered pornographic, offensive, illegal or discriminatory. I understand that to do so may constitute a disciplinary offence and in some cases a criminal offence.
- Images of students and/or staff will only be taken, 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 Headteacher.
- 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 or the school into disrepute and understand that material I publish online may be taken into consideration when I apply for a job.
- I will support and promote the school's Online Safety policy and help students to be safe and responsible in their use of ICT and related technologies.

User Signature
I agree to follow this code of conduct & to support the safe use of ICT throughout the school

Signature _____________________________Date ______________

Full Name ___________________________________ (printed)

Appendix C: Current Legislation

Keeping Children Safe in Education, 2024 update

All staff should undergo safeguarding and child protection training (including online safety) at induction. There have been some changes to Parts 1 and 2 of KCSIE but none relate directly to online safety.

Prevent Duty, 2015

Schools have a requirement to identify sites that may appear innocuous but attempt to display harmful content to children and to keep accurate records of exactly who does what, whether the internet requests are allowed or blocked. This helps to identify the signs of radicalisation, whether explicit or significant as part of a pattern of behaviour. These signs are then passed on through the child protection team in line with our child protection policy

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.

https://www.legislation.gov.uk/ukpga/2003/42/contents

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.

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.

https://www.legislation.gov.uk/ukpga/2000/23/contents

Human Rights Act 1998
https://www.legislation.gov.uk/ukpga/1998/42/contents

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.

https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted

The Telecommunications (Lawful Business Practice)

(Interception of Communications) Regulations 2000

https://www.legislation.gov.uk/uksi/2000/2699/contents/made

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 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.

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.

Online Safety Act 2023
This Act provides for a new regulatory framework which has the general purpose of making the use of internet services regulated by this Act safer for individuals in the United Kingdom. To achieve that purpose, this Act (among other things)—

> (a)imposes duties which, in broad terms, require providers of services regulated by this Act to identify, mitigate and manage the risks of harm (including risks which particularly affect individuals with a certain characteristic) from—
>
> > (i)illegal content and activity, and
> > (ii)content and activity that is harmful to children, and
>
> (b)confers new functions and powers on the regulator, OFCOM.

https://www.legislation.gov.uk/ukpga/2023/50/contents

Data (Use and Access) Act 2025

The (Data Use and Access) Act 2025 ("DUA Act") came into force in August 2025 and is a legislative change intended to simplify data protection laws such as the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 (DPA) and the Privacy and Electronic Communications Regulations (PECR). Although the changes do not overhaul the current data protection legislation significantly in the main, the changes affect how individual's personal data will be processed.

https://www.legislation.gov.uk/ukpga/2025/18/introduction