Central Region Schools Trust

Founded by the RSA

ONLINE SAFETY POLICY & ACCEPTABLE USE AGREEMENTS

Recommended by:	Head of IT & Data
Ratified by:	F&R Committee
Signed:	
Position on the Board:	**Chair to F&R Committee**
Ratification Date	19.09.2024
Next Review:	Autum 2025
Policy Tier (Central/Hub/School):	Central

1. Introduction

Central Region Schools Trust (the Trust) is fully committed to enhancing and expanding our efforts in protecting the students under our care, in strict accordance with the law. We recognise that today's children are growing up in an increasingly intricate and interconnected world, seamlessly navigating both online and offline environments. While this offers countless positive and exciting opportunities, it also exposes them to various challenges and risks. Therefore, we are determined to ensure that our schools equip children with comprehensive knowledge, enabling them to utilise the internet and technology in the safest, most responsible, and respectful manner possible, thus enabling them to fully reap the vast benefits of the online world.

This Online Safety Policy outlines the commitment of the Trust to ensuring a safe and secure online environment for all students, staff, parents/carers, and stakeholders within the Trust. The policy aims to provide guidelines, procedures, and education to promote responsible online behaviours, protect against online risks, and foster a culture of digital citizenship.

The Trust aims to:

- have robust processes in place to ensure the online safety of students, staff, volunteers, trustees, and governors.
- deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology.
- establish clear mechanisms to identify, intervene and escalate an incident, where appropriate.

2. Roles and Responsibilities

This policy applies to all trustees, governors, staff, trainees and students in the Trust. Any breach of this policy will be considered an offence and the Trust's disciplinary procedures could be invoked.

As a matter of best practice, other agencies and individuals working with the Trust, and who have access to personal information, will be expected to read and comply with this policy. It is expected that departments or individuals who are responsible for dealing with external bodies will take the responsibility for ensuring that such bodies sign a contract which, among other things, will include an agreement to abide by this policy.

The local academy governing board and trust board are responsible for:

- Ensuring that this policy is effective and complies with relevant laws and statutory guidance.
- Ensuring the DSL's remit covers online safety.
- Ensuring their own knowledge of online safety issues is up to date.
- Ensuring all staff undergo safeguarding and child protection training, including online safety, at induction.
- Ensuring that there are appropriate filtering and monitoring systems in place.
- Ensuring that all relevant school policies have an effective approach to planning for, and responding to, online challenges and hoaxes embedded within them.

The Principal and/or Head of School are responsible for:

- Ensuring that online safety is a running and interrelated theme throughout the school's policies and procedures, including in those related to the curriculum, teacher training and safeguarding.

- Supporting the DSL and the deputy DSL by ensuring they have enough time and resources to carry out their responsibilities in relation to online safety.
- Ensuring staff receive regular, up-to-date, and appropriate online safety training and information as part of their induction and safeguarding training.
- Ensuring online safety practices are audited and evaluated.
- Supporting staff to ensure that online safety is embedded throughout the curriculum so that all students can develop an appropriate understanding of online safety.
- Organising engagement with parents/carers to keep them up to date with current online safety issues and how the school is keeping students safe.
- Working with the DSL and IT Services Teams to conduct yearly reviews of this policy.
- Working with the DSL and local academy governing board to update this policy on an annual basis.

The Designated Safeguarding Lead (DSL) is responsible for:

- Taking the lead responsibility for online safety in the school.
- Acting as the named point of contact within the school on all online safeguarding issues.
- Undertaking training so they understand the risks associated with online safety and can recognise additional risks that students with SEND face online.
- Liaising with relevant members of staff on online safety matters, e.g., the SENCO and IT Services Teams.
- Ensuring online safety is recognised as part of the Trust's/school's safeguarding responsibilities and that a coordinated approach is implemented.
- Ensuring safeguarding is considered in the school's approach to remote learning.
- Ensuring appropriate referrals are made to external agencies, as required.
- Working closely with the police during police investigations.
- Keeping up to date with current research, legislation, and online trends.
- Coordinating the school's participation in local and national online safety events, e.g., Safer Internet Day.
- Establishing a procedure for reporting online safety incidents and inappropriate internet use, both by students and staff.
- Ensuring all members of the school community understand the reporting procedure.
- Maintaining records of reported online safety concerns as well as the actions taken in response to concerns.
- Monitoring online safety incidents to identify trends and any gaps in the Trust's/school's provision and using this data to update the Trust's/school's procedures.
- Reporting to the local academy governing board about online safety on a termly basis.
- Working with the Principal/Head of School and IT Services Teams to conduct yearly reviews of this policy.
- Take a lead responsibility for Online Safety including understanding the filtering and monitoring systems in place.

The IT Services Team with oversight by the Head of IT are responsible for:

- Providing technical support in the development and implementation of the Trust's/school's online safety policies and procedures.
- Implementing appropriate security measures as directed by the Principal/Head of School.
- Regularly updating the school's filtering and monitoring systems to align with current requirements.
- Collaborating with the DSL and Principal/Head of School to conduct reviews of this policy on a yearly basis, ensuring its relevance and effectiveness.

All staff members (and volunteers) are responsible for:

- Taking responsibility for the security of ICT systems and electronic data they use or have access to.
- Modelling good online behaviours.
- Maintaining a professional level of conduct in their personal use of technology.
- Having an awareness of online safety issues.
- Ensuring they are familiar with, and understand, the indicators that students may be unsafe online.
- Reporting concerns in line with the Trust's/school's reporting procedure.
- Where relevant to their role, ensuring online safety is embedded in their teaching of the curriculum.

Students are responsible for:

- Adhering to the Acceptable Use Agreement and other relevant policies.
- Seeking help from school staff if they are concerned about something they or a peer have experienced online.
- Reporting online safety incidents and concerns in line with the procedures within this policy.
- Managing their own online safety

Parents/Carers are expected to:

- Notify a member of staff or the Principal/Head of School of any concerns or queries regarding this policy
- Ensure their child understands the issues surrounding online safety
- Ensure their child has read, understood, and agreed to the terms on acceptable use of the Trust's/school's ICT systems and internet.

3. **Education and Awareness**

The purpose of using technology in school is to raise educational standards, promote student achievement, support the professional work of staff, and enhance school management functions.

Students are encouraged to use technology within school and outside of school to support their learning. It is important therefore to teach them the skills of using it appropriately, knowing and understanding the risks to allow them to take care of their own safety and security.

Students will be taught to:

- use technology safely and respectfully
- recognise acceptable and unacceptable behaviour
- report concerns about content, contact, conduct and commerce
- protect their online identity and privacy
- understand how changes in technology affect safety

Safe use of social media and internet will also be covered in other subjects where relevant. The school will use the curriculum and assemblies to raise students' awareness of the dangers that can be encountered online and may also invite speakers to talk to students about this.

Online Safety Education for Students

The purpose of using technology in school is to raise educational standards, promote student achievement, support the professional work of staff, and enhance school management functions.

Students are encouraged to use technology within school and outside of school to support their learning. It is important therefore to teach them the skills of using it appropriately, knowing and understanding the risks to allow them to take care of their own safety and security.

Students will be taught to:
- use technology safely and respectfully
- recognise acceptable and unacceptable behaviour
- report concerns about content, contact, conduct and commerce
- protect their online identity and privacy
- understand how changes in technology affect safety

Safe use of social media and internet will also be covered in other subjects where relevant. The school will use the curriculum and assemblies to raise students' awareness of the dangers that can be encountered online and may also invite speakers to talk to students about this.

Online Safety Education for Parents/Carers
Parents/Carers will receive information regarding online safety through school newsletters or other communications home and in information via school websites. This policy will also be available to parents/carers on our websites.

If parents/carers have any queries or concerns in relation to online safety, these should be raised in the first instance with the Principal/Head of school and/or DSL.

4. **Cyberbullying**
Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship may involve an imbalance of power.

Prevention and Response to Cyberbullying
To help prevent cyber-bullying, we ensure all students understand what it is and what to do if they become aware of it happening to them or others. We will ensure that students know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with students, explaining the reasons why it occurs, the forms it may take and what the consequences can be.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate, or harmful material has been spread among students, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will consider local safeguarding procedures when deciding whether an incident should be reported to the police if it involves illegal material and will work with external services if it is deemed necessary to do so.

Examination of Electronic Devices

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on students' electronic devices, including mobile phones, iPads, and other tablet devices, where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- cause harm, and/or
- disrupt teaching, and/or
- break any of the school rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

- delete that material, or
- retain it as evidence (of a criminal offence or a breach of school discipline), and/or
- report it to the police

Any searching of students will be carried out in line with the DfE's latest guidance on screening, searching and confiscation.

Any complaints about searching for or deleting inappropriate images or files on students' electronic devices will be dealt with through the Trust's complaints procedure.

5. **Cybercrime Awareness**

Cybercrime is criminal activity committed using computers and/or the internet. It is broadly categorised as either 'cyber-enabled' (crimes that can happen off-line but are enabled at scale and at speed on-line) or 'cyber dependent' (crimes that can be committed only by using a computer). Cyber-dependent crimes include.

- unauthorised access to computers (illegal 'hacking'), for example accessing a school's computer network to look for test paper answers or change grades awarded.
- denial of Service (Dos or DDoS) attacks or 'booting'. These are attempts to make a computer, network, or website unavailable by overwhelming it with internet traffic from multiple sources; and
- making, supplying, or obtaining malware (malicious software) such as viruses, spyware, ransomware, botnets, and Remote Access Trojans with the intent to commit further offence, including those above

The network manager and Trust Head of IT will ensure the appropriate level of security protection procedures are in place, to safeguard systems, staff, and learners. The effectiveness of these procedures will be reviewed periodically to keep up with evolving cyber-crime technologies. If there are concerns about a student in this area, the designated safeguarding lead (or a deputy), will follow the correct safeguarding procedure and may consider referring into the Cyber Choices programme.

6. Use of Mobile Technologies

The Trust and all its schools recognise that mobile phones are a feature of modern society. Many students have unlimited and unrestricted access to the internet via mobile phone networks (i.e., 3G, 4G and 5G). This access means some children could, whilst at school, bully or sexually harass their peers via their mobile and smart technology, share indecent images consensually and non-

consensually (often via large chat groups) and view and share pornography and other harmful content.

For these reasons, we have a dedicated mobile phone principles policy available via our websites.

7. Online Safety during Remote Learning

In our Trust the safety and well-being of our students during remote learning is one of our top priorities. We recognise the critical role of online safety in creating a secure and positive learning environment, even in remote learning settings. Therefore, we adhere to the principles outlined in the Trust's Staff Code of Conduct when it comes to online teaching. This comprehensive policy covers the acceptable use of technology, maintaining appropriate staff-student relationships, and responsible communication, including the use of social media.

As we navigate remote learning, it is essential to establish clear reporting routes for children working online, ensuring that they can raise any concerns they may have. In addition to reporting routes back to the school, children have access to age-appropriate support services from reputable organisations such as Childline, which provides valuable support, the UK Safer Internet Centre, which facilitates reporting and removal of harmful online content, and CEOP, which offers guidance on making reports about online abuse.

During this engagement, staff members will likely communicate with parents/carers. We emphasise the importance of ensuring children's online safety in these communications. It is particularly vital for parents/carers to be fully informed about the online activities their children are engaging in, including the specific websites they will be accessing, and to be clear about the individuals from the school, if any, with whom their child will interact online.

Parents/carers may choose to complement the school's online offerings with support from online companies or individual tutors. In such cases, we strongly encourage parents/carers to select reputable organisations or individuals who can provide evidence of their safety and trustworthiness when working with children.

While there is no expectation for teachers to live stream or provide pre-recorded videos, for those who choose to do so, it is crucial that they familiarise themselves with the Trust's guidance on conducting remote live sessions. Please refer to the Trust's Live Lessons document for detailed instructions on how to ensure effective and safe online teaching practices.

Teaching from home presents unique challenges distinct from the traditional classroom setting. Therefore, teachers should strive to find a quiet or private room or area for communicating with students and parents/carers. Additionally, when broadcasting a lesson or creating a recording, teachers should consider the background and ensure that their attire is appropriate. It is essential to share and agree upon guidance.

8. Incident Response and Reporting

In the event of a student misusing the Trust's/school's ICT systems or the internet, we will adhere to the procedures outlined in the behaviour policy. The appropriate action will be determined based on the specific incident's individual circumstances, nature, and severity, ensuring a proportional response.

If a staff member misuses the school's ICT systems, the internet, or their personal device in a manner that constitutes misconduct, the matter will be addressed in accordance with the staff

disciplinary procedures. The course of action will be determined based on the specific incident's individual circumstances, nature, and seriousness.

In instances involving illegal activity or content, or any other significant incidents, the school will carefully consider whether it is necessary to report the matter to the police.

8. Staff Training and Professional Development
As part of their induction, all new staff members will undergo comprehensive safeguarding training, which includes education on safe internet usage and online safeguarding matters such as cyberbullying, cybercrime, and the risks associated with online radicalisation.

To ensure ongoing awareness and preparedness, all staff members will receive refresher training at least once per academic year as part of their safeguarding training. They will also receive relevant updates as needed, which may be conveyed through emails, e-bulletins, or staff meetings.

The designated safeguarding lead, as well as the deputy safeguarding leads, will undertake child protection and safeguarding training, which incorporates online safety, at least every two years. They will actively update their knowledge and skills in the field of online safety at regular intervals, with a minimum frequency of once per year.

Governors will also receive training on safe internet usage and online safeguarding matters as part of their safeguarding training program.

Volunteers, if applicable, will receive appropriate training and updates to ensure their understanding of safeguarding procedures.

For further information on safeguarding training, including details on specific programs and initiatives, please refer to our Safeguarding policy, which is available on our websites.

9. How to report an online safety incident
The Trust takes online safety incidents seriously and is committed to promptly addressing and resolving any concerns. We encourage all students, staff, parents/carers, and stakeholders to report any online safety incidents they encounter. This includes instances of cyberbullying, inappropriate content, grooming, or any other online behaviour that raises concerns about the safety and well-being of individuals within our school community.

To ensure a swift and appropriate response, we have established clear procedures for reporting online safety incidents:

Students: Students are encouraged to report any online safety incidents to a trusted adult, such as a teacher, member of the support staff, or the designated safeguarding lead. They can also use the reporting routes established within the school, which may include anonymous reporting options. It is important for students to provide as much information as possible, including details of the incident, individuals involved, and any supporting evidence.

Staff: Staff members who become aware of an online safety incident should report it to the designated safeguarding lead or their line manager. They should provide a detailed account of the incident, including relevant information and any supporting evidence they may have. Staff members should not attempt to handle the incident themselves but should rely on the established reporting procedures.

Parents/Carers: Parents/carers are encouraged to report any online safety incidents involving their child promptly. They should contact the school directly, either by speaking to their child's teacher, the designated safeguarding lead, or any other relevant staff member. Parents/carers should provide specific details about the incident, including dates, times, individuals involved, and any supporting evidence they may have.
Upon receiving a report, the designated safeguarding lead, or a designated member of staff, will initiate a thorough investigation into the online safety incident. This may involve gathering additional information, consulting relevant parties, and taking appropriate action to address the incident and support those involved.

We assure all individuals making reports that they will be treated with respect and their concerns will be taken seriously. It is essential to remember that reporting an online safety incident is a responsible and courageous act, contributing to maintaining a safe and secure online environment for all members of our school community.

10. **Appendix 1: e-Safety information, Advice and Support**

Numerous resources are available to support schools, colleges, and parents/carers in ensuring children's online safety. While not exhaustive, the following list serves as a valuable starting point:

Support for parents/carers.

- Internet Matters – a not-for-profit organisation set up to empower parents/carers to keep children safe in the digital world. Their support for parents includes a range of downloadable guides covering subjects such as transition to secondary school, Vlogging & livestreaming, online gaming, and cyberbullying.
- NSPCC - includes a range of resources to help parents/carers keep children safe when they're using the internet, social networks, apps, games and more.
- Parent Info - from CEOP and Parent Zone, Parent Info is a website for parents/carers covering all the issues amplified by the internet. It is a free service which helps schools engage parents/carers with expert safety advice, endorsed by the National Crime Agency's CEOP command. This website provides expert information across a range of online harms.
- Parent Zone - offers a range of resources for families, to help them meet the challenges of the digital age, including parent guides on the latest digital trends and platforms.
- Common Sense Media - Independent reviews, age ratings, & other information about all types of media including games, apps, films, and books.
- Let's Talk About It has advice for parents/carers to keep children safe from online radicalisation.
- Childnet offers a toolkit to support parents/carers of children of any age to start discussions about their online life, to set boundaries around online behaviour and technology use, and to find out where to get more help and support
- London Grid for Learning has support for parents/carers to keep their children safe online, including tips to keep primary aged children safe online

Support for students

- BBC Own It – Support for young people to take control of their online life, including help and advice, skills, and inspiration on topics such as friendships and bullying, safety, and self-esteem. Free app available.
- Childline – includes information for students on sexting, gaming, grooming, bullying, porn, relationships.
- Think U Know – age-appropriate advice for staying safe when using a tablet, mobile phone, or computer.
- Disrespect Nobody - Home Office advice on healthy relationships, including sexting and pornography

Support and Resources for Schools: Government Guidance

- Keeping Children Safe in Education - Statutory guidance for schools and colleges on safeguarding children and safer recruitment.
- Teaching online safety in schools - DfE advice outlining how schools can ensure their students understand how to stay safe and behave online as part of existing curriculum requirements.
- Behaviour and discipline in schools - Guidance for school leaders and staff on developing a school behaviour policy, and a checklist of actions to take to encourage good behaviour.

- Searching, screening and confiscation at school - Guidance explaining the powers schools have to screen and search students, and to confiscate items they find.
- Educateagainsthate - Practical advice for parents/carers, teachers, and governors on protecting children from extremism and radicalisation.
- The use of social media for online radicalisation - A briefing note for schools on how social media is used to encourage travel to Syria and Iraq.
- CEOP Think U Know Programme: Online safety education programme from the National Crime Agency's CEOP Command which aims to safeguard children from sexual abuse and exploitation. Education resources and online advice for children aged 4 – 18, expert and support and professional development for the children's workforce. Signposts to the NCA's Click CEOP service for children to report concerns related to sexual abuse.
- National Centre for Computing Education (NCCE) has been set up to support the teaching of computing education throughout schools and colleges in England, giving teachers the subject knowledge and skills to establish computing as a core part of the curriculum. To help primary and secondary schools teach the safety and security aspects of the National Curriculum Computing Programme of Study, the National Centre for Computing Education's resource repository and professional development courses cover objectives from the Education for Connected World framework. The resource repository's lesson plans will include links to the framework, as well as specific activities for non-specialist teachers.
- UK Council for Internet Safety - The UK Council for Internet Safety expands the scope of the UK Council for Child Internet Safety to achieve a safer online experience for all users, particularly groups who suffer disproportionate harms. The website has useful resources for schools and parents/carers to help keep children safe online including Education for a Connected World – a framework describes the Digital knowledge and skills that children and young people should have the opportunity to develop at different ages and stages of their lives. It highlights what a child should know in terms of current online technology, its influence on behaviour and development, and what skills they need to be able to navigate it.
- UK Chief Medical Officers' advice for parents/carers on children and young people's screen and social media use, published February 2019.
- National Organisations: Support, Resources and Training for Schools
- National Online Safety – Specialist online safety training courses for staff, parents/carers, and children along with resources for use in the classroom.
- The Anti-Bullying Alliance - A coalition of organisations and individuals, working together to stop bullying and create safer environments in which children and young people can live, grow, play and learn. Their website includes a range of tools and resources to support schools prevent and tackle cyberbullying.
- Childnet - a children's charity and has a wide range of practical resources freely available, covering all online safety issues, and which are available for teachers working with children of all ages, including children with SEN.
- The Diana Award – a charity running several different projects aimed at reducing bullying in schools. Their resource section has information to help schools tackle cyberbullying along with resources from there Be Strong Online Ambassador programme – a peer-led initiative which aims to empower young people to increase the digital resilience of their peers.

- DotCom Digital - a free resource for schools, created by children with Essex Police and the National Police Chief Council Lead for Internet Intelligence and Investigations, to be launched October 2019. The resource aims to prevent young people becoming victims of online grooming, radicalisation, exploitation and bullying by giving them the confidence to recognise warning signs and reach out to an adult for help.
- The Hopes and Streams report by London Grid for Learning has themed chapters that include links to online resources and ideas for tackling the issues raised.
- Internet Matters – a not-for-profit organisation set up to empower parents/carers to keep children safe in the digital world, they also have a dedicated section of their website for professionals which includes resources to support staff training, whole school programmes and policies and a parent pack to help schools engage with /carers about online safety.
- Internet Watch Foundation – an internet hotline for the public and IT professionals to report potentially criminal online content, including child sexual abuse images online.
- NSPCC learning – includes a range of safeguarding and child protection teaching resources, advice and training for schools and colleges.
- Parent Zone's dedicated school zone - includes a range of resources to support teachers educate their students on how to stay safe online, what to do if they find themselves in an uncomfortable situation and how to build their digital resilience.
- PSHE Association - the national body for Personal, Social, Health and Economic (PSHE) education. Their programme of study for PSHE education aims to develop skills and attributes such as resilience, self-esteem, risk-management, team working and critical thinking. They also have many guides about how to teach specific topics.
- UK Safer Internet Centre –a partnership between Childnet International, Internet Watch Foundation and SWGfL to promote the safe and responsible use of technology for young people. Their website includes a range of practical resources and support for schools including: 360 degree safe - a free to use self-review tool for schools to assess their wider online safety policy and practice. A Helpline – This helpline was established to support those working with children across the UK with online safety issues. Operated by SWGfL, it can be contacted at 0344 381 4772 and helpline@saferinternet.org.uk. Safer Internet Day - The UK Safer Internet Centre organise Safer Internet Day for the UK and each year develops a range of materials from assemblies to lesson plans, posters to quizzes, for each Key Stage, to address a key online safety issue.
- Be Internet Legends - Be Internet Legends from Google and Parentzone a free internet safety curriculum with PSHE accredited lesson plans and teaching resources for Key Stage 2 students

11. **Appendix 2: Staff (and volunteer) Acceptable Use Agreement**

The Trust is a professional organisation with responsibility for children's safeguarding and so it is important that staff take all possible and necessary measures to protect data and information systems from infection, unauthorised access, damage, loss, abuse, and theft. All members of staff have a responsibility to use the Trust's computer systems in a professional, lawful, and ethical manner. To ensure that members of staff are fully aware of their professional responsibilities when using information technology and the systems, they are asked to read this 'Staff (and volunteer) Acceptable Use Agreement" before accessing the network or using any Trust devices.

This is not an exhaustive list, and all members of staff are reminded that IT use should be consistent with the Trust's ethos, other appropriate policies, and the law. Any misuse of technology by a member of staff will not be taken lightly and should be reported to the relevant Principal, Head of school, Executive Principal or Chief Operating Officer for any necessary further action to be taken.

The Trust offers a wide variety of constantly improving and developing IT resources to our staff and students. All staff have a responsibility to support and monitor the safe use of the relevant school/s network, internet, and email by students. Any member of staff who requires further training or support should inform their line manager and contact the Trust's IT Services Team for further training.

Please read this document carefully. Before you login to the Trust's network or use a device within the Trust, you confirm you have read, understood, and agree to comply with this 'Staff (and volunteer) Acceptable Use Agreement".

1. **General Guidance**

- Before accessing any Trust or School IT system, I will ensure I have completed National Cyber Security Centre training.
- Staff should not leave a device logged in where it could be viewed or accessed by another user without first locking the screen. On a Windows device this can be done by pressing ⊞ Win + L or Ctrl + Alt + Delete on the keyboard. Other operating systems may vary so please check with the IT Services team if you are unsure how to lock your device.
- Staff must use strong passwords for all Trust and School systems, ensuring they are private, at least 8 characters long, and contain a mix of upper/lowercase letters, numbers, and symbols. Passwords should not include personal details or significant dates, must be unique for each system, and must not be written down (e.g., on post-it notes).
- Staff should not add, amend, or delete any personal data held on students or staff, including their own data. If any amendments are necessary, a request should be raised to the Trust HR Department.
- Staff should use the internet appropriately and teach and support students to do the same. The internet gives access to both desirable and undesirable material that may be unsuitable for students despite advanced filtering. Separate internet filtering policies are applied to staff and students. Staff should ensure they do not:
    - visit websites, make, post, download, upload or pass on, material, remarks, proposals, or comments that contain or relate to:
        - pornography (including child pornography)
        - the promotion of discrimination, racial or religious hatred, including any form of extremist propaganda or any site promoting radicalisation
        - the promotion of illegal acts
        - gaming, betting, or gambling
        - a potential breach of any Trust or school policies
        - anything which exposes children in the care of the Trust and school to danger

        - any information which may be offensive to colleagues
    - breach copyright law

Incidents of unacceptable use will be treated as a disciplinary issue. If abuse is found to be repeated, flagrant or habitual, the matter will be treated as a serious disciplinary issue.

2. Using technology in school

- I will only use ICT systems which have been permitted for my use by the IT Services team, Principal or Head of School (e.g., Computers, Laptops, Tablets).
- I will ensure any personal devices (including desktop computers and mobile devices) used to access my Trust/school provided email account or work documents meet the following requirements:
    - protected using a strong password only know to yourself
    - contain up-to-date anti-virus protection
    - the device is encrypted (to protect data from unauthorised access)
- I will only use the approved IT accounts that have been provided to me by the IT Services Team.
- I will not use personal emails to send and receive staff or student personal data, or sensitive data relating to the Trust.
- I understand that my Trust/school email address, account, and its contents remain the property of the Trust.
- I will delete any chain letters, spam, and other emails from unknown sources without opening them.
- I will not attempt to bypass any filtering and/or security systems put in place by the Trust/school.
- I understand that my Trust/school account and its contents may be transferred to my line manager or other senior members of staff to support business continuity.
- I will not store any personal information on the Trust's/school's computer system that is unrelated to Trust/school activities, such as personal photographs, files, or financial information.
- I will not share sensitive personal data with any other staff, students or third parties unless explicit consent has been received and if required, a DPIA has been completed in accordance with UK GDPR.
- I will exercise caution when using a projector or interactive screen to ensure no sensitive or personal information is displayed to other users. (E.g., Emails and MIS information are not projected and use extended screen mode where possible)
- I will ensure that any personal data of students, staff or parents/carers is kept in accordance with current UK GDPR regulations. This means that all personal data will be obtained and processed fairly and lawfully, only kept for specific purposes, held no longer than necessary, and will be kept private and secure with appropriate security measures in place, whether used in the workplace, hosted online, or accessed remotely. Any sensitive data should not be removed from the internal network and systems. Any data which is removed from a school site should be encrypted by a method approved by the Trust/school.
- I will ensure that I obtain permission prior to accessing teaching materials from unapproved sources.
- I will only use the internet for personal use during out-of-school hours, including break and lunch times, providing this material is appropriate and suitable in accordance with this policy.
- I understand that my use of all Trust/school information systems and internet are monitored and recorded to ensure policy compliance.
- I will not search for, view, download, upload or transmit any explicit or inappropriate material when using the internet.
- I will not share school-related passwords with students, staff or third parties unless permission has been given for me to do so by the Trust Head of IT or a Trust Network Manager.
- I will not install any software onto school ICT systems unless authorised to do so by the Trust Head of IT or a Trust Network Manager.
- I will ensure any school-owned device is protected by anti-virus software and that I check this on a weekly basis.

- I will ensure Trust or School related data is stored in my designated cloud storage area by default and regularly check to ensure any sync software is working. (E.g., For Windows devices, this will be OneDrive for individual documents and SharePoint for shared documents. OneDrive sync software will appear in the taskbar and hovering over the taskbar icon will detail the sync status).
- I will not use USB sticks, or removable media devices unless necessary, and with approval from the IT Services Team. I will keep any school-related information stored on these secure by using encryption.
- I will only store sensitive personal data where it is necessary, and the device has been encrypted.
- Trust/school owned information systems must be used appropriately. I understand that the Computer Misuse Act 1990 makes the following criminal offences: to gain unauthorised access to computer material; to gain unauthorised access to computer material with intent to commit or facilitate commission of further offences or to modify computer material without authorisation.
- If I have any queries or questions regarding safe and professional practice online either at work or off site, then I will raise them with the IT Services Team and line manager.

3. Mobile devices

- I will only use school-owned mobile devices for educational purposes.
- I will adhere to my school's specific mobile phone policy concerning the use of personal mobile phones within school premises or classrooms.
- If work calls are taken within school, I will ensure this is taken in a private area if the conversation is of a sensitive nature.
- I will not use personal devices to take photographs or videos of students or staff.
- I will seek permission from the Principal or Head of School before any school-owned mobile device is used to take images or recordings.
- I will not use mobile devices to send inappropriate messages, images, or recordings.
- I will ensure that personal and school-owned mobile devices do not contain any inappropriate or illegal content.
- I will not access the Wi-Fi system using personal mobile devices unless permission has been given by the Principal, Head of School or IT Services Team.
- I will not use personal devices to communicate with students or parents/carers.
- I will not store any images or videos of students, staff, or parents/carers on any mobile device unless consent has been sought from the individual(s) in the images or videos.
- In line with the above, I will only process images or videos of students, staff, or parents/carers for the activities for which consent has been sought.
- I will take measures to ensure that any school data stored on personal mobile devices is protected through strong authentication and encryption. I will allow the IT Services Team to erase and wipe data from my device in the event of loss or as part of exit procedures.

4. Social media and online professionalism

- It is recognised that staff and students may at some time produce and publish materials on a website associated with the Trust and/or school.
    - No materials will be published on the internet, which contain any unacceptable images, language, or content. Infringement of this rule will be taken as a serious disciplinary issue.
    - No materials will be published on the internet that reveal the identity of any student without explicit consent, in accordance with GDPR and other school policies.
    - Materials produced by students, and photographs of students, will not be published on the internet without parental approval or approval from the appropriate carer/social worker; and
    - No materials will be published on the internet without approval by the Chief Executive officer, relevant Head of School or Principal, Chief Operating Officer, or Trust Head of IT.

- If I am representing the school online, e.g., through blogging or on a school social media account, I will express neutral opinions and will not disclose any confidential information regarding the school, or any information that may affect its reputability.
- I will not use any school-owned mobile devices to access personal social networking sites, unless it is beneficial to the material being taught; I will gain permission from the Principal or Head of School before accessing the site.
- I will not communicate with students or parents/carers over personal social networking sites.
- I will not accept friend requests, follow requests, or seek to add any of the following on my personal social media account/s:
    - current student/s or past student/s under the age of 18
    - parents/guardians of current student/s or past student/s under the age of 18
    - I will declare to the school Principal or CEO without delay if I have any of the above as a connection on my current social media account/s.
- I will ensure that appropriate privacy settings are applied to all social networking sites I use, to safeguard personal information and prevent unauthorised access by students, guardians, or other unintended parties.
- I will not publish any comments or posts about the school on any social networking sites which may affect the school's reputability.
- I will not post or upload any defamatory, objectionable, copyright-infringing, or private material, including images and videos of students, staff, or parents/carers, on any online website.
- I will not post or upload any images and videos of students, staff, or parents/carers on any online website without consent from the individual(s) in the images or videos.
- I will not give my home address, phone number, mobile number, social networking details or email addresses to students or parents/carers – any contact with parents/carers will be done through authorised school contact channels.

5. Working from home/remotely

- I will adhere to the principles of the UK GDPR when working from home.
- I will ensure I obtain permission from the Principal or Head of School and DPO before any personal data is transferred from a school-owned device to a personal device.
- I will ensure any data transferred from a school-owned device to a personal device is encrypted.
- I will ensure any sensitive personal data is not transferred to a personal device unless completely necessary and I have authorisation from the IT Services Team. If required, I ensure that this is encrypted.
- I will ensure any personal devices (including desktop computers and mobile devices) used to access my Trust/school provided email account or work documents meet the following requirements:
    - protected using a strong password only know to yourself
    - contain up-to-date anti-virus protection
    - the device is encrypted (to protect data from unauthorised access)
- I will ensure that no unauthorised individuals, including family members or friends, have access to my work devices or accounts when working from home or remotely.
- I will adhere to the school's Online Safety Policy when transporting school equipment and data. Devices must be always kept secure to prevent loss or theft. Laptops and other equipment should not be left visible in vehicles and must be stored securely.

6. Training

- Before accessing any Trust or School IT system, I will ensure I have completed National Cyber Security Centre training.
- I will ensure I participate in any online safety training offered to me and will remain up to date with current developments in social media and the internet.
- I will ensure that I allow the IT Services Team and DPO to undertake regular audits to identify any areas of need I may have in relation to training.

- I will ensure I employ methods of good practice and act as a role model for students when using the internet and other digital devices.
- I will promote e-safety with the students in my care and will help them to develop a responsible attitude to safety online, system use and to the content they access or create.
- I will ensure that I deliver any training to students as required.

7. Reporting concerns, issues, or misuse

- I will ensure that I adhere to any responsibility I have for monitoring, as outlined in the Online Safety Policy, e.g., to monitor students' internet usage.
- If I suspect a computer or system has been damaged or affected by a virus or other malware, or if I suspect cyber-attack, I will report this to the IT Services Team immediately.
- I will report all incidents of concern regarding student's online safety to the DSL and Senior IT Technician/Network Manager/Head of IT as soon as possible. I will report any accidental access, receipt of inappropriate materials, filtering breaches or unsuitable websites to the Chief Executive officer, relevant head of school, Chief Operating Officer, Head of IT, Network Manager or Senior IT Technician as soon as possible.
- I will ensure that I report any misuse by students or staff members breaching the procedures outlined in this agreement to the Principal or Head of School and Trust Head of IT.
- I understand that my use of the Trust IT Systems and the internet will be monitored and recognise the consequences if I breach the terms of this agreement.
- I understand that the principal or head of school may decide to take disciplinary action against me, in accordance with the Disciplinary Policy and Procedure, if I breach this agreement.

The Trust/school reserves the right to monitor the use of information systems, including Internet access and email interception, to ensure compliance with our trust/school policies, including our Trust Online Safety Policy and Trust Data Protection Policy. In cases where unauthorised or inappropriate use of the information system is suspected, or if there is evidence of unacceptable or inappropriate behaviour, the Trust/school will initiate the disciplinary procedure. If there is reason to believe that the system is being used for criminal activities or storing unlawful content, the matter will be reported to the appropriate law enforcement agencies.

I acknowledge that I have read and understood the Staff (and volunteer) Acceptable Use Agreement and ensure that I will abide by each principle.

12. **Appendix 3: Student Acceptable Use Agreement for Secondary Schools**

The Trust understands the benefits technology can have on enhancing the curriculum and students' learning; however, we must ensure that students respect school property and use technology appropriately. To achieve this, we have created this acceptable use agreement which outlines our expectations of students when using technology, whether this is on personal or school devices and on or off the school premises.

Any misuse of technology will not be taken lightly and should be reported to the Principal or Head of School for any necessary further action to be taken. Please read this document carefully. Before you login to the Trust's network or use a device within school, you confirm you have read, understood, and agree to comply with this 'Student IT Acceptable Use Policy'.

1. Aims of this policy

The aims of this Acceptable Use Policy are:

- To ensure that students may benefit from the learning opportunities offered by the Trust' network and internet resources in a safe and effective manner.
- To protect the Trust's IT infrastructure from misuse and attack.

2. The Trust and its' schools undertake to:

- Prioritise Data Protection and adhere to strict guidelines on the use of personal or sensitive information.
- Provide a safe and productive digital learning environment.
- Provide students with training in internet safety.
- Supervise students' network and internet access wherever possible.
- Monitor students' network and internet activities using software systems.
- Provide internet filtering to minimise the risk of inappropriate material being accessed.
- Ensure there is a secure and regular backup of student data wherever possible.
- Ensure that robust and up to date virus detection and security systems are in place to protect students' data.
- Only publish students' projects, artwork, or schoolwork on the website/internet in line with the agreed Trust policy.

3. Important information for all students:

- Use of IT Facilities is forbidden unless supervised by a member of staff.
- Network and Internet access are considered a Trust resource and a privilege. If this Acceptable Use Policy is not adhered to, this privilege will be withdrawn, and appropriate sanctions will be imposed.
- Designated staff can review student files and communications to ensure that the system is being used responsibly. They also have the right to access computer storage areas and accounts.
- Designated members of staff can remotely view a student's computer screen at any time, without them knowing, to ensure compliance and appropriate use of the Trust's network.
- Students are subject to the provisions of the Copyright, Designs and Patents Act 1988.
- The Trust and its schools will provide information on the following legislation relating to use of the Trust's network, which teachers, students and parents/carers should familiarise themselves with: The Data Protection Act 2018; Video Recordings Act 1989; Copyright, Designs and Patents Act 1988; and Computer Misuse Act 1990.

4. Using technology in school

- I will only use ICT systems, e.g., computers, laptops, and tablets, which my class teacher has given me permission to use.

- I will only use the approved email account that has been provided to me by the IT Services Team.
- I will not store or use any personal data relating to a student or staff member for non-school related activities. If I have any queries about storing or using personal data, I will speak to my class teacher.
- I will delete any chain letters, spam, and other emails from unknown senders without opening them.
- I will not attempt to release viruses or carry out any other malicious practice that contravenes the Computer Misuse Act 1990.
- I will not access or alter other people's folders, work, or files without permission.
- I will ensure that I get permission from my class teacher before accessing learning materials, e.g., source documents, from unapproved sources.
- I will report any attempts of people contacting me outside the Trust and school community to a member of staff immediately.
- I will not pass personal information on (like real names or addresses) to anyone on the internet.
- I will report any damaged IT equipment (accidentally or otherwise) to the supervising member of staff immediately.
- I will not eat or drink in any room where there is IT equipment.
- I will always ask for permission to use the printer and will not print unnecessarily. I also understand that any print jobs I send to the printers are monitored and recorded.
- I will only use the internet for personal use during out-of-school hours, including break and lunchtimes. During school hours, I will use the internet for schoolwork only.
- I will not reveal my password to anyone or use someone else's username or password. I understand I'm responsible for the actions of anyone who is using my username and password, so must immediately tell a member of staff if they suspect that someone else has this information.
- I will not install any software onto school ICT systems unless instructed to do so by my class teacher.
- I will not use USB sticks, or removable media devices without approval from the IT Services Team and I will keep all school-related information stored on these secure by using encryption.
- I will adhere to the online safety guidelines I have been taught.
- I will only use the school's ICT facilities to:
    - Complete homework and coursework.
    - Prepare for lessons and exams.
    - Undertake revision and research.
    - Gather or process information for extracurricular activities, e.g., creating the school newsletter.
- I will not attempt to bypass the Trust's internet filters. Violation of this is a serious offence.
- I will not use the school's ICT facilities to access, download, upload, send, receive, view or display any of the following:
    - Illegal material and/or sexually explicit content
    - Any content that could constitute a threat, bullying or harassment, or anything negative about other persons or the school
    - Content relating to a person's sexual orientation, gender, religion, race, disability, or age
    - Gaming, Betting, or online gambling
    - Content which may adversely affect the reputation of any organisation (including the school) or person, whether they are known to be true or false

- Any material which breaches copyright law.

5. Mobile devices

- I will use school-owned mobile devices, e.g., laptops and tablets, for educational purposes only.
- I will adhere to my school's specific mobile phone policy concerning the use of personal mobile phones within school premises or classrooms.
- I will seek permission from my class teacher before a school-owned mobile device is used to take images or recordings.
- I will not use any mobile devices to take pictures of fellow students unless I have their consent.
- I will not use any mobile devices to send inappropriate messages, images, or recordings.
- I will ensure that personal and school-owned mobile devices do not contain any inappropriate or illegal content.
- I will not access the Wi-Fi system using a personal device unless permission has been given by the class teacher and IT Services Team.
- I will not take or store images or videos of staff members on any mobile device, regardless of whether or not it is school owned.

6. Use of Trust laptops and portable devices

In some circumstances, students may be allowed to borrow the Trust's laptops or other IT equipment. The student and parent/carer will need to sign a document to accept responsibility of the device. All devices must be returned to the relevant school once the student leaves, when the student no longer needs it, or when it is requested back by a member of staff.

- You will not leave the device unattended, and it must be securely stored when not in use.
- You will not install any software on the device without consulting the Trust's IT Services Team first.
- Any technical issues with the device must be reported immediately to a member of the Trust's IT Services team.
- Students MUST NOT attempt to disassemble the device or attempt to fix it themselves.
- If you lose your device, or if it is stolen, you must report it immediately to your form teacher, or a member of the Trust's IT Services team.
- If you accidently damage the device, you must report it immediately to your form teacher, or a member of the Trust's IT Services team.
- No modifications will be made to the device. All hardware changes and installations must be completed by a member of the Trust's IT Services team.
- The device is to be used for educational purposes only.
- It is recommended that data stored on the device is backed up regularly. Should an issue develop with the device, the Trust's IT Services team may be required to reset the device to its original factory settings. Such a procedure will result in the irretrievable loss of all information stored on the device.
- While the device remains Trust property, the usage of the device will be monitored.
- On acceptance of the device, the student and parent/carer accept responsibility for the safe keeping of the device and if it is damaged beyond repair or lost, they will be invoiced for the full cost of the replacement.

7. Social Media

- I will not use any school-owned mobile devices to access personal social networking platforms.
- I will not communicate or attempt to communicate with any staff member over personal social networking platforms.

- I will not accept or send 'friend' or 'follow' requests from or to any staff member over personal social networking platforms.
- I will ensure that I apply the necessary privacy settings to any social networking sites.
- I will not publish any comments or posts about the school on any social networking platforms which may affect the school's reputation.
- I will not post or upload any defamatory, objectionable, copyright-infringing, or private material, including images and videos of students, staff, or parents/carers, on any online website.
- I will not post any material online that:
    - Is offensive.
    - Is private or sensitive.
    - Infringes copyright laws.
    - Damages the school's reputation.
    - Is an image or video of any staff member, parent, or nonconsenting student.

8. Reporting concerns or misuse

- I will ensure that I report any misuse or breaches of this agreement by students or staff members to the Head of School and Trust Head of IT
- I understand that my use of the Trust IT Systems and the internet will be monitored and recognise the consequences if I breach the terms of this agreement.
- I understand that the Principal or Head of School may decide to take disciplinary action against me in accordance with the school's Behavioural Policy if I breach this agreement.
- I'm aware of the CEOP report button and know when to use it.

I acknowledge that I have read and understood the Student Acceptable Use Agreement (Secondary School) and ensure that I will abide by each principle.

13. Appendix 4: Student Acceptable Use Agreement for Primary Schools

The Trust knows that it can be fun to use technology as part of your learning experience. We want everyone to be able to use technology, like computers and tablets, but it is important that you are safe when you are using them.

We have created this agreement to help you understand how to be safe when you are using technology. Please read this carefully and sign your name to show that you understand your responsibilities when using technology. Ask your teacher if there is something that you do not understand.



I will:

- ✓ Only use technology, such as a computer, when a teacher has given me permission.
- ✓ Only use technology for the reason I have been asked to use it.
- ✓ Only use the internet when a teacher has given me permission.
- ✓ Ask for help when I have a problem using the technology.
- ✓ Look after the device and try not to damage it.
- ✓ Tell the teacher if my device is not working or damaged.
- ✓ Tell the teacher if I think someone else is not using technology safely or correctly.
- ✓ Tell the teacher if I see something online that I think is inappropriate or that makes me upset.

I will not:

- ✘ Tell another student my username and password.
- ✘ Share personal information, such as my age and where I live, about myself or my friends online.
- ✘ Access social media, such as Facebook and WhatsApp.
- ✘ Speak to strangers on the internet.
- ✘ Take photos of myself or my friends using a school device.

Please read each statement and provide a tick to show that you agree, and then write your name below.

- ☐ I understand why it is important to use technology safely and correctly.
- ☐ I understand my responsibilities when using technology.

- ☐ I understand that I may not be allowed to use technology if I do not use it safely and correctly.
- ☐ I will always follow these rules.

Student name (please print): _____
Date: _____

Parent/Carer name (please print): _____
Parent/Carer signature: _____
Date: _____