The Robert Carre Trust

Online Safety Policy

Contents:

Statement of intent

The Robert Carre Trust understands that using online services is an important aspect of raising educational standards, promoting student achievement, and enhancing teaching and learning. The use of online services is embedded throughout the schools; therefore, there are a number of controls in place to ensure the safety of students and staff.

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

- **Content**: Being exposed to illegal, inappropriate or harmful material, e.g., pornography, fake news, self-harm and suicide, and discriminatory or extremist views.
- **Contact**: Being subjected to harmful online interaction with other users, e.g., peer pressure, commercial advertising, and adults posing as children or young adults with the intention to groom or exploit children.
- **Conduct**: Personal online behaviour that increases the likelihood of, or causes, harm, e.g., sending and receiving explicit messages, and cyberbullying.
- **Commerce**: Risks such as online gambling, inappropriate advertising, phishing and/or financial scams.

The measures implemented to protect students and staff revolve around these areas of risk. The Trust has created this policy with the aim of ensuring appropriate and safe use of the internet and other digital technology devices by all students and staff.

Legal framework

This policy has due regard to all relevant legislation and guidance including, but not limited to, the following:

- Voyeurism (Offences) Act 2019
- The UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- DfE (2021) 'Harmful online challenges and online hoaxes'
- DfE (2022) 'Keeping children safe in education 2022'
- DfE (2023) 'Teaching online safety in school'
- DfE (2022) 'Searching, screening and confiscation'
- Department for Digital, Culture, Media and Sport and UK Council for Internet Safety (2020) 'Sharing nudes and semi-nudes: advice for education settings working with children and young people'
- UK Council for Child Internet Safety (2020) 'Education for a Connected World – 2020 edition'
- National Cyber Security Centre (2018) 'Small Business Guide: Cyber Security'

This policy operates in conjunction with the following Trust/School policies:

- RCT Social Media Policy
- RCT Managing Allegations of Abuse Against Staff Policy
- RCT ICT – Acceptable Use (Staff) Policy
- RCT ICT – Acceptable Use Policy (AUP) Students and Media Forms
- RCT Security Policy
- RPA Cyber Response Plan
- RCT Child Protection and Safeguarding Policy
- RCT Anti-Harassment and Bullying Policy (Student)
- RCT Anti-Harassment and Bullying Policy (Staff)
- RCT Bring Your Own Device (BYOD) Policy
- RCT Mobile Phone and Device Policy
- RCT Code of Conduct for Employees

- CGS Behaviour Policy
- KSHS Behaviour Policy
- RCT Staff Disciplinary Policy and Procedures
- RCT Data Protection (GDPR) Policy
- RCT Bring Your Own Device (BYOD) Policy
- RCT Mobile Phone and Devices Policy

Roles and responsibilities

The Trustees will be responsible for:

- Ensuring that this policy is effective and complies with relevant laws and statutory guidance.
- Ensuring the DSLs' remit covers online safety.
- Reviewing this policy on an annual basis.
- 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 and at regular intervals.
- 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 Executive Headteacher and/or Headteacher will be responsible for:

- Ensuring that online safety is a running and interrelated theme throughout the Trust's policies and procedures, including in those related to the curriculum, teacher training and safeguarding.
- Supporting the DSLs and the deputy DSLs 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.
- Organising engagement with parents to keep them up-to-date with current online safety issues and how the trust is keeping students safe.
- Working with the DSLs and ICT to conduct light-touch reviews of this policy.
- Working with the DSLs and Trustees to update this policy on an annual basis.

The DSLs will be responsible for:

- Taking the lead responsibility for online safety in the schools.
- 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 ICT.
- Ensuring online safety is recognised as part of the Trust's safeguarding responsibilities and that a coordinated approach is implemented.
- Ensuring safeguarding is considered in the school's approach to remote learning.
- Establishing a procedure for reporting online safety incidents and inappropriate internet use, both by students and staff, and ensuring all members of the Trust community understand this 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 provision, and using this data to update the Trust's procedures.

- Reporting to the Trustees/Governors about online safety on a termly basis.
- Working with the Executive Headteacher and/or Headteacher and ICT to conduct light-touch reviews of this policy.
- Working with the Executive Headteacher and/or Headteacher and the Trust to update this policy on an annual basis.

ICT will be responsible for:

- Providing technical support in the development and implementation of the Trust's online safety policies and procedures.
- Implementing appropriate security measures as directed by the Executive Headteacher and/or Headteacher.
- Ensuring that the Trust's filtering and monitoring systems are updated as appropriate.
- Working with the DSL and Executive Headteacher and/or Headteacher to conduct light-touch reviews of this policy.

All staff members will be 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 reporting procedure.
- Where relevant to their role, ensuring online safety is embedded in their teaching of the curriculum.

Students will be responsible for:

- Adhering to the Acceptable Use Agreement and other relevant policies.
- Seeking help from 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 online safety

All staff will be aware that technology is a significant component in many safeguarding and wellbeing issues affecting young people, particularly owing to the rise of social media and the increased prevalence of children using the internet.

The DSLs have overall responsibility for the schools' approach to online safety, with support from other Senior Leaders where appropriate, and will ensure that there are strong processes in place to handle any concerns about students' safety online. The DSLs should liaise with the police or children's social care services for support responding to harmful online sexual behaviour.

The importance of online safety is integrated across all school operations in the following ways:

- Staff and governors receive regular training
- Staff receive regular email updates regarding online safety information and any changes to online safety guidance or legislation

The Personal Development Curriculum covers online safety. **Handling online safety concerns**

Any disclosures made by students to staff members about online abuse, harassment or exploitation, whether they are the victim or disclosing on behalf of another child, will be handled in line with the Child Protection and Safeguarding Policy.

Staff will be aware that harmful online sexual behaviour can progress on a continuum, and appropriate and early intervention can prevent abusive behaviour in the future. Staff will also acknowledge that students displaying this type of behaviour are often victims of abuse themselves and should be suitably supported.

The victim of online harmful sexual behaviour may ask for no one to be told about the abuse. The DSLs will consider whether sharing details of the abuse would put the victim in a more harmful position, or whether it is necessary in order to protect them from further harm. Ultimately the DSLs will balance the victim's wishes against their duty to protect the victim and other young people. The DSLs and other appropriate staff members will meet with the victim's parents to discuss the safeguarding measures that are being put in place to support their child and how the report will progress.

Confidentiality will not be promised, and information may be still shared lawfully, for example, if a DSL decides that there is a legal basis under UK GDPR such as the public task basis whereby it is in the public interest to share the information. If the decision is made to report abuse to children's social care or the police against the victim's wishes, this must be handled extremely carefully – the reasons for sharing the information should be explained to the victim and appropriate specialised support should be offered.

Concerns regarding a staff member's online behaviour are reported to the Executive Headteacher and/or Headteacher who decides on the best course of action in line with the relevant policies. If the concern is about the Executive Headteacher and/or Headteacher, it is reported to the Chair of the Trustees.

Concerns regarding a student's online behaviour are reported to the DSL, who investigates concerns with relevant staff members, e.g., the Executive Headteacher and/or and ICT, and manages concerns in accordance with relevant policies depending on their nature, e.g., the Behaviour Policy and Child Protection and Safeguarding Policy.

Where there is a concern that illegal activity has taken place, the Executive Headteacher and/or Headteacher contacts the police.

The school avoids unnecessarily criminalising students, e.g., calling the police, where criminal behaviour is thought to be inadvertent and as a result of ignorance or normal developmental curiosity, e.g., a student has taken and distributed indecent imagery of themselves. The DSL will decide in which cases this response is appropriate and will manage such cases in line with the Child Protection and Safeguarding Policy.

All online safety incidents and the schools' response are recorded by the DSLs.

Cyberbullying

Cyberbullying can include, but is not limited to, the following:

- Threatening, intimidating or upsetting text messages
- Threatening or embarrassing pictures and video clips sent via mobile phone cameras
- Silent or abusive phone calls or using the victim's phone to harass others, to make them think the victim is responsible
- Threatening or bullying emails, possibly sent using a pseudonym or someone else's name
- Unpleasant messages sent via instant messaging
- Unpleasant or defamatory information posted to blogs, personal websites and social networking sites, e.g., Facebook
- Abuse between young people in intimate relationships online i.e., teenage relationship abuse

- Discriminatory bullying online i.e., homophobia, racism, misogyny/misandry.

The Trust will be aware that certain students can be more at risk of abuse and/or bullying online, such as LGBTQ+ students and students with SEND.

Cyberbullying against students or staff is not tolerated under any circumstances. Incidents of cyberbullying are dealt with quickly and effectively wherever they occur in line with the Anti-Harassment and Bullying Policy.

Child-on-child sexual abuse and harassment

Students may also use the internet and technology as a vehicle for sexual abuse and harassment. Staff will understand that this abuse can occur both in and outside of school, off and online, and will remain aware that students are less likely to report concerning online sexual behaviours, particularly if they are using websites that they know adults will consider to be inappropriate for their age.

The following are examples of online harmful sexual behaviour of which staff will be expected to be aware:

- Threatening, facilitating or encouraging sexual violence
- Upskirting, i.e., taking a picture underneath a person's clothing without consent and with the intention of viewing their genitals, breasts or buttocks
- Sexualised online bullying, e.g., sexual jokes or taunts
- Unwanted and unsolicited sexual comments and messages
- Consensual or non-consensual sharing of sexualised imagery
- Abuse between young people in intimate relationships online, i.e., teenage relationship abuse

All staff will be aware of and promote a zero-tolerance approach to sexually harassing or abusive behaviour, and any attempts to pass such behaviour off as trivial or harmless. Staff will be aware that allowing such behaviour could lead to a school culture that normalises abuse and leads to students becoming less likely to report such conduct.

Staff will be aware that creating, possessing, and distributing indecent imagery of other children, i.e., individuals under the age of 18, is a criminal offence, even where the imagery is created, possessed, and distributed with the permission of the child depicted, or by the child themselves.

The Trust will be aware that interactions between the victim of online harmful sexual behaviour and the alleged perpetrator(s) are likely to occur over social media following the initial report, as well as interactions with other students taking "sides", often leading to repeat harassment. The school will respond to these incidents in line with the Child Protection and Safeguarding Policy, the Anti-Harassment and Bullying Policies and the Social Media Policy.

The Trust will respond to all concerns regarding online child-on-child sexual abuse and harassment, regardless of whether the incident took place on the school premises or using school-owned equipment. Concerns regarding online child-on-child abuse will be reported to the DSL, who will investigate the matter in line with the Child Protection and Safeguarding Policy, the Anit-Harassment and Bullying Policies.

Grooming and exploitation

Grooming is defined as the situation whereby an adult builds a relationship, trust and emotional connection with a child with the intention of manipulating, exploiting and/or abusing them.

Staff will be aware that grooming often takes place online and that students who are being groomed are commonly unlikely to report this behaviour for many reasons, e.g., the student

may have been manipulated into feeling a strong bond with their groomer and may have feelings of loyalty, admiration, or love, as well as fear, distress and confusion.

Due to the fact students are less likely to report grooming than other online offences, it is particularly important that staff understand the indicators of this type of abuse. DSLs will ensure that online safety training covers online abuse, the importance of looking for signs of grooming, and what the signs of online grooming are, including:

- Being secretive about how they are spending their time online.
- Having an older boyfriend or girlfriend, usually one that does not attend the school and whom their close friends have not met.
- Having money or new possessions, e.g., clothes and technological devices, that they cannot or will not explain.

Child sexual exploitation (CSE) and child criminal exploitation (CCE)

Although CSE often involves physical sexual abuse or violence, online elements may be prevalent, e.g., sexual coercion and encouraging children to behave in sexually inappropriate ways through the internet. In some cases, a student may be groomed online to become involved in a wider network of exploitation, e.g., the production of child pornography or forced child prostitution and sexual trafficking.

CCE is a form of exploitation in which children are forced or manipulated into committing crimes for the benefit of their abuser, e.g., drug transporting, shoplifting and serious violence. While these crimes often take place in person, it is increasingly common for children to be groomed and manipulated into participating through the internet.

Where staff have any concerns about students with relation to CSE or CCE, they will bring these concerns to the DSLs without delay, who will manage the situation in line with the Child Protection and Safeguarding Policy.

Radicalisation

Radicalisation is the process by which a person comes to support terrorism and extremist ideologies associated with terrorist groups. This process can occur through direct recruitment, e.g., individuals in extremist groups identifying, targeting and contacting young people with the intention of involving them in terrorist activity, or by exposure to violent ideological propaganda. Children who are targets for radicalisation are likely to be groomed by extremists online to the extent that they believe the extremist has their best interests at heart, making them more likely to adopt the same radical ideology.

Staff members will be aware of the factors which can place certain students at increased vulnerability to radicalisation, as outlined in the Child Protection and Safeguarding Policy. Staff will be expected to exercise vigilance towards any students displaying indicators that they have been, or are being, radicalised.

Where staff have a concern about a student relating to radicalisation, they will report this to the DSLs without delay, who will handle the situation in line with the Child Protection and Safeguarding Policy.

Mental health

Staff will be aware that online activity both in and outside of school can have a substantial impact on a student's mental state, both positively and negatively. The DSL will ensure that training is available to help ensure that staff members understand popular social media sites and terminology, the ways in which social media and the internet in general can impact mental health, and the indicators that a student is suffering from challenges in their mental health.

Online hoaxes and harmful online challenges
For the purposes of this policy, an **"online hoax"** is defined as a deliberate lie designed to seem truthful, normally one that is intended to scaremonger or to distress individuals who come across it, spread on online social media platforms.

For the purposes of this policy, **"harmful online challenges"** refers to challenges that are targeted at young people and generally involve users recording themselves participating in an online challenge, distributing the video through social media channels and daring others to do the same. Although many online challenges are harmless, an online challenge becomes harmful when it could potentially put the participant at risk of harm, either directly as a result of partaking in the challenge itself or indirectly as a result of the distribution of the video online – the latter will usually depend on the age of the student and the way in which they are depicted in the video.

Where staff suspect there may be a harmful online challenge or online hoax circulating amongst students in the school, they will report this to the relevant DSL immediately.

The DSL will conduct a case-by-case assessment for any harmful online content brought to their attention, establishing the scale and nature of the possible risk to students, and whether the risk is one that is localised to the school or the local area, or whether it extends more widely across the country. Where the harmful content is prevalent mainly in the local area, the DSL will consult with the LA about whether quick local action can prevent the hoax or challenge from spreading more widely.

Prior to deciding how to respond to a harmful online challenge or hoax, the DSL and the headteacher will decide whether each proposed response is:

- In line with any advice received from a known, reliable source, e.g., the UK Safer Internet Centre, when fact-checking the risk of online challenges or hoaxes.
- Careful to avoid needlessly scaring or distressing students.
- Not inadvertently encouraging students to view the hoax or challenge where they would not have otherwise come across it, e.g., where content is explained to younger students but is almost exclusively being shared amongst older students.
- Proportional to the actual or perceived risk.
- Helpful to the students who are, or are perceived to be, at risk.
- Appropriate for the relevant students' age and developmental stage.
- Supportive.
- In line with the Child Protection and Safeguarding Policy.

Where the DSL's assessment finds an online challenge to be putting students at risk of harm, they will ensure that the challenge is directly addressed to the relevant students, e.g., those within a particular age range that is directly affected or individual students at risk where appropriate.

The DSLs and Executive Headteacher and/or Headteacher will only implement a Trust-wide approach to highlighting potential harms of a hoax or challenge when the risk of needlessly increasing students' exposure to the risk is considered and mitigated as far as possible.

Cyber-crime

Cyber-crime is criminal activity committed using computers and/or the internet. There are two key categories of cyber-crime:

- **Cyber-enabled** – these crimes can be carried out offline; however, are made easier and can be conducted at higher scales and speeds online, e.g.. fraud, purchasing and selling of illegal drugs, and sexual abuse and exploitation.
- **Cyber-dependent** – these crimes can only be carried out online or by using a computer, e.g., making, supplying or obtaining malware, illegal hacking, and 'booting',

which means overwhelming a network, computer or website with internet traffic to render it unavailable.

The Trust will factor into its approach to online safety the risk that students with a particular affinity or skill in technology may become involved, whether deliberately or inadvertently, in cyber-crime. Where there are any concerns about a student's use of technology and their intentions with regard to using their skill and affinity towards it, the DSL will consider a referral to the Cyber Choices programme, which aims to intervene where children are at risk of committing cyber-crime and divert them to a more positive use of their skills and interests.

The DSL and Executive Headteacher and/or Headteacher will ensure that students are taught, throughout the curriculum, how to use technology safely, responsibly and lawfully.

Online safety training for staff

The DSL ensures that all safeguarding training given to staff includes elements of online safety, including how the internet can facilitate abuse and exploitation. All staff will be made aware that students are at risk of abuse, by their peers and by adults, online as well as in person, and that, often, abuse will take place concurrently via online channels and in daily life.

Online safety and the curriculum

Online safety is embedded throughout the curriculum; however, it is particularly addressed in the following subjects:

- RSE
- PSHE
- Citizenship
- ICT
- Tutor Time Sessions

Online safety teaching is always appropriate to students' ages and developmental stages.

Students are taught the underpinning knowledge and behaviours that can help them to navigate the online world safely and confidently regardless of the device, platform or app they are using. The underpinning knowledge and behaviours students learn through the curriculum include the following:

- How to evaluate what they see online
- How to recognise techniques used for persuasion
- Acceptable and unacceptable online behaviour
- How to identify online risks
- How and when to seek support
- Knowledge and behaviours that are covered in the government's online media literacy strategy

The online risks students may face online are always considered when developing the curriculum. The risks that are considered and how they are covered in the curriculum can be found in appendix A of this policy.

The DSLs will be involved with the development of the school's online safety curriculum. Students will be consulted on the online safety curriculum, where appropriate, due to their unique knowledge of the kinds of websites they and their peers frequent and the kinds of behaviours in which they engage online.

Relevant members of staff, e.g., the SENCO will work together to ensure the curriculum is tailored so that students who may be more vulnerable to online harms, e.g., students with SEND and LAC, receive the information and support they need.

The Trust will also endeavour to take a more personalised or contextualised approach to teaching about online safety for more susceptible children, and in response to instances of harmful online behaviour from students.

Teachers will review external resources prior to using them for the online safety curriculum, to ensure they are appropriate for the cohort of students.

External visitors may be invited into school to help with the delivery of certain aspects of the online safety curriculum. The Executive Headteacher and/or Headteacher and DSLs will decide when it is appropriate to invite external groups into school and ensure the visitors selected are appropriate.

Before conducting a lesson or activity on online safety, the teacher and DSL will consider the topic that is being covered and the potential that students in the class have suffered or may be suffering from online abuse or harm in this way. The DSL will advise the staff member on how to best support any student who may be especially impacted by a lesson or activity. Lessons and activities will be planned carefully so they do not draw attention to a student who is being or has been abused or harmed online, to avoid publicising the abuse.

During an online safety lesson or activity, the teacher will ensure a safe environment is maintained in which students feel comfortable to say what they feel and ask questions, and are not worried about getting into trouble or being judged.

If a staff member is concerned about anything students raise during online safety lessons and activities, they will make a report in line with the Child Protection and Safeguarding Policy.

If a student makes a disclosure to a member of staff regarding online abuse following a lesson or activity, the staff member will follow the reporting procedure outlined in the Child Protection and Safeguarding Policy.

Use of technology in the classroom

A wide range of technology will be used during lessons, including the following:

- Computers
- Laptops
- Tablets
- Intranet
- Email
- Cameras
- Smartphones, (occasional use)

Prior to using any websites, tools, apps or other online platforms in the classroom, or recommending that students use these platforms at home, the teacher will review and evaluate the resource. Teachers will ensure that any internet-derived materials are used in line with copyright law.

Students will be supervised when using online materials during lesson time – this supervision is suitable to their age and ability.

Use of smart technology

While the school recognises that the use of smart technology can have educational benefits, there are also a variety of associated risks which the school will ensure it manages.

Students will be educated on the acceptable and appropriate use of personal devices and will use technology in line with the Trust's ICT Acceptable Use Agreement for Students and the Trust's Mobile Phone and Devices Policy.

Staff will use all smart technology and personal technology in line with the school's ICT Acceptable Use (Staff) Policy and the RCT Bring Your Own Device (BYOD) Policy.

The school recognises that students' unlimited and unrestricted access to the internet via mobile phone networks means that some students may use the internet in a way which breaches the school's acceptable use of ICT agreement for students.

Inappropriate use of smart technology may include:

- Using mobile and smart technology to sexually harass, bully, troll or intimidate peers.
- Sharing indecent images, both consensually and non-consensually.
- Viewing and sharing pornography and other harmful content.

Students will not be permitted to use smart devices or any other personal technology whilst in the classroom, without the teacher's permission.

Where it is deemed necessary, the Trust will ban student's use of personal technology whilst on school site.

Where there is a significant problem with the misuse of smart technology among students, the school will discipline those involved in line with the schools' Behaviour Policies.

The schools will hold assemblies, where appropriate, which address any specific concerns related to the misuse of smart technology and outline the importance of using smart technology in an appropriate manner.

The Trust will seek to ensure that it is kept up to date with the latest devices, platforms, apps, trends and related threats.

The Trust will consider the 4Cs (content, contact, conduct and commerce) when educating students about the risks involved with the inappropriate use of smart technology and enforcing the appropriate disciplinary measures.

Educating parents

The Trust will work in partnership with parents to ensure students stay safe online at school and at home. Parents will be provided with information about the Trust's approach to online safety and their role in protecting their children. Parents will be signposted to a copy of the Acceptable Use Agreement at the beginning of each academic year and are encouraged to go through this with their child to ensure their child understands the document and the implications of not following it.

Parents will be made aware of the various ways in which their children may be at risk online, including, but not limited to:

- Child sexual abuse, including grooming.
- Exposure to radicalising content.
- Sharing of indecent imagery of students, e.g., sexting.
- Cyberbullying.
- Exposure to age-inappropriate content, e.g., pornography.
- Exposure to harmful content, e.g., content that encourages self-destructive behaviour.

Parents will be informed of the ways in which they can prevent their child from accessing harmful content at home, e.g., by implementing parental controls to block age-inappropriate content.

Parental awareness regarding how they can support their children to be safe online will be raised in the following ways:

- Parents' evenings
- Twilight training sessions
- Newsletters
- Online resources

Internet access

Students, staff and other members of the school community will only be granted access to the school's internet network once they have read and signed the Acceptable Use Agreement. A record will be kept of users who have been granted internet access.

All members of the Trust community will be encouraged to use the Trust's internet network, instead of 3G, 4G and 5G networks, as the network has appropriate filtering and monitoring to ensure individuals are using the internet appropriately.

Filtering and monitoring online activity

The Trust will ensure the Trust's ICT network has appropriate filters and monitoring systems in place. The Trust will ensure 'over blocking' does not lead to unreasonable restrictions as to what students can be taught with regards to online teaching and safeguarding.

The Executive Headteacher and/or Headteacher and ICT will undertake a risk assessment to determine what filtering and monitoring systems are required. The filtering and monitoring systems the school implements will be appropriate to students' ages, the number of students using the network, how often students access the network, and the proportionality of costs compared to the risks. ICT will report any concerns raised on the filtering and monitoring systems to ensure they are effective and appropriate.

Reports of inappropriate websites or materials will be made to the ICT team immediately, who will investigate the matter and makes any necessary changes.

Deliberate breaches of the filtering system will be reported to the DSL and ICT team, who will escalate the matter appropriately. If a student has deliberately breached the filtering system, they will be disciplined in line with the Behaviour Policies. If a member of staff has deliberately breached the filtering system, they will be disciplined in line with the Disciplinary Policy and Procedure.

If material that is believed to be illegal is accessed, inadvertently or deliberately, this material will be reported to the appropriate agency immediately, e.g., the Internet Watch Foundation (IWF), CEOP and/or the police.

The Trust's network and Trust-owned devices will be appropriately monitored. All users of the network and Trust-owned devices will be informed about how and why they are monitored. Concerns identified through monitoring will be reported to the DSL who will manage the situation in line with the Child Protection and Safeguarding Policy.

Network security

Technical security features, such as anti-virus software, will be kept up-to-date and managed by ICT team. The Trust's Firewall is managed by emPSN and their partners.

Staff and students will be advised not to download unapproved software or open unfamiliar email attachments, and will be expected to report all malware and virus attacks to ICT team.

All members of staff will have their own unique usernames and private passwords to access the Trust's systems. Students will be provided with their own unique username and private passwords. Staff members and students will be responsible for keeping their passwords private. Passwords will have a minimum and maximum length and require a mixture of letters, numbers and symbols to ensure they are as secure as possible. Passwords will expire after 40 days, after which users will be required to change them.

Users will not be permitted to share their login details with others and will not be allowed to log in as another user at any time. If a user is found to be sharing their login details or otherwise mistreating the password system, the Executive Headteacher and/or Headteacher will be informed and will decide the necessary action to take.

Users will be required to lock access to devices and systems when they are not in use.

Full details of the Trust's network security measures can be found in the ICT Policies.

Emails

Access to and the use of emails will be managed in line with the RCT Data Protection (GDPR) Policy and Acceptable Use Agreements.

Staff and students will be given approved Trust email accounts and will only be able to use these accounts at school and when doing school-related work outside of school hours. Prior to being authorised to use the email system, staff and students must agree to and sign the Acceptable Use Agreement. Personal email accounts will not be permitted to be used on the school site. Any email that contains sensitive or personal information will only be sent using secure and encrypted email.

Staff members and students will be required to block spam and junk mail, and report the matter to ICT. The Trust's monitoring system can detect inappropriate links, malware and profanity within emails – staff and students will be made aware of this. Chain letters, spam and all other emails from unknown sources will be deleted without being opened. ICT will organise regular training where they explain what a phishing email and other malicious emails might look like – this assembly will includes information on the following:

- How to determine whether an email address is legitimate
- The types of address a phishing email could use
- The importance of asking "does the email urge you to act immediately?"
- The importance of checking the spelling and grammar of an email

Social networking

The use of social media by staff and students will be managed in line with the Trust's Social Media Policy.

The school website

The Executive Headteacher and/or Headteacher will be responsible for the overall content of the school website – they will ensure the content is appropriate, accurate, up-to-date and meets government requirements.

Use of devices

Staff members and students will be issued with Trust-owned devices to assist with their work, where necessary. Requirements around the use of devices can be found in the Trust's ICT policies.

The use of personal devices on the school premises and for the purposes of school work will be managed in line with the ICT Bring Your Own Devices Policy.

Remote learning

All remote tutoring will be delivered in line with the school's Online tutoring Protocol and Guidance, as set out at Appendix B to this policy. This protocol specifically sets out how online safety will be considered when delivering remote education

Monitoring and review

The Trust recognises that the online world is constantly changing; therefore, the DSL, ICT and the Executive Headteacher and/or Headteacher conduct light-touch reviews of this policy to evaluate its effectiveness.

The Trust, Executive Headteacher and/or Headteacher and DSLs will review this policy in full on an annual basis and following any online safety incidents.

Any changes made to this policy are communicated to all members of the school community.

Adopted by the Trustees on 18th March 2025

Next Review due September 2025 (annually)

Appendix A

Online harms and risks – curriculum coverage

Subject area	Description and teaching content	Curriculum area the harm or risk is covered in
How to navigate the internet and manage information		
Age restrictions	Some online activities have age restrictions because they include content which is not appropriate for children under a specific age. Teaching will include the following: • That age verification exists and why some online platforms ask users to verify their age • Why age restrictions exist • That content that requires age verification can be damaging to under-age consumers • What the age of digital consent is (13 for most platforms) and why it is important	This risk or harm will be covered in the following curriculum areas: • Health education • Computing • Personal Development time including Tutor time sessions and PSHE
How content can be used and shared	Knowing what happens to information, comments or images that are put online. Teaching will include the following: • What a digital footprint is, how it develops and how it can affect students' futures • How cookies work • How content can be shared, tagged and traced • How difficult it is to remove something once it has been shared online • What is illegal online, e.g. youth-produced sexual imagery (sexting)	This risk or harm will be covered in the following curriculum areas: • RSE • Computing • Personal Development time including Tutor time sessions and PSHE
Disinformation, misinformation and hoaxes	Some information shared online is accidentally or intentionally wrong, misleading or exaggerated. Teaching will include the following: • Disinformation and why individuals or groups choose to share false information in order to deliberately deceive • Misinformation and being aware that false and misleading information can be shared inadvertently. • Malinformation and understanding that some genuine information can be published with the deliberate intent to harm, e.g., releasing private information or photographs	This risk or harm will be covered in the following curriculum areas: • RSE • Computing • PSHE & Citizenship • Personal Development time including Tutor time

	• Online hoaxes, which can be deliberately and inadvertently spread for a variety of reasons • That the widespread nature of this sort of content can often appear to be a stamp of authenticity, making it important to evaluate what is seen online • How to measure and check authenticity online • The potential consequences of sharing information that may not be true	sessions and PSHE
Fake websites and scam emails	Fake websites and scam emails are used to extort data, money, images and other things that can either be used by the scammer to harm the person targeted or sold on for financial, or other, gain. Teaching will include the following: • How to recognise fake URLs and websites • What secure markings on websites are and how to assess the sources of emails • The risks of entering information to a website which is not secure • What students should do if they are harmed, targeted, or groomed as a result of interacting with a fake website or scam email • Who students should go to for support • The risk of 'too good to be true' online offers, advertising and fake product sales designed to persuade people to part with money for products and services that do not exist	This risk or harm will be covered in the following curriculum areas: • RSE • Computing • Personal Development time including Tutor time sessions and PSHE
Online fraud	Fraud can take place online and can have serious consequences for individuals and organisations. Teaching will include the following: • What identity fraud, scams and phishing are • That online fraud can be highly sophisticated and that anyone can be a victim • How to protect yourself and others against different types of online fraud • How to identify 'money mule' schemes and recruiters • The risk of online social engineering to facilitate authorised push payment fraud, where a victim is tricked into sending a payment to the criminal • The risk of sharing personal information that could be used by fraudsters • That children are sometimes targeted to access adults' data • What 'good' companies will and will not do when it comes to personal details	This risk or harm will be covered in the following curriculum areas: • RSE • Computing • Personal Development time including Tutor time sessions and PSHE

	• How to report fraud, phishing attempts, suspicious websites and adverts	
Password phishing	Password phishing is the process by which people try to find out individuals' passwords so they can access protected content. Teaching will include the following: • Why passwords are important, how to keep them safe and that others might try to get people to reveal them • How to recognise phishing scams • The importance of online security to protect against viruses that are designed to gain access to password information • What to do when a password is compromised or thought to be compromised	This risk or harm will be covered in the following curriculum areas: • RSE • Computing • Personal Development time including Tutor time sessions and PSHE
Personal data	Online platforms and search engines gather personal data – this is often referred to as 'harvesting' or 'farming'. Teaching will include the following: • How cookies work • How data is farmed from sources which look neutral • How and why personal data is shared by online companies • How students can protect themselves and that acting quickly is essential when something happens • The rights children have with regards to their data • How to limit the data companies can gather	This risk or harm will be covered in the following curriculum areas: • RSE • Computing • Personal Development time including Tutor time sessions and PSHE
Persuasive design	Many devices, apps and games are designed to keep users online for longer than they might have planned or desired. Teaching will include the following: • That the majority of games and platforms are designed to make money, and that their primary driver is to encourage people to stay online for as long as possible to encourage	This risk or harm will be covered in the following curriculum areas: • Health education • Computing • Personal Development

	them to spend money or generate advertising revenue • How notifications are used to pull users back online	time including Tutor time sessions and PSHE
Privacy settings	Almost all devices, websites, apps and other online services come with privacy settings that can be used to control what is shared. Teaching will include the following: • How to find information about privacy settings on various sites, apps, devices and platforms • That privacy settings have limitations	This risk or harm will be covered in the following curriculum areas: • RSE • Computing • Personal Development time including Tutor time sessions and PSHE
Targeting of online content	Much of the information seen online is a result of some form of targeting. Teaching will include the following: • How adverts seen at the top of online searches and social media have often come from companies paying to be on there and different people will see different adverts • How the targeting is done • The concept of clickbait and how companies can use it to draw people to their sites and services	This risk or harm will be covered in the following curriculum areas: • RSE • Computing • Personal Development time including Tutor time sessions and PSHE
How to stay safe online		
Online abuse	Some online behaviours are abusive. They are negative in nature, potentially harmful and, in some cases, can be illegal. Teaching will include the following: • The types of online abuse, including sexual harassment, bullying, trolling and intimidation • When online abuse can become illegal • How to respond to online abuse and how to access support • How to respond when the abuse is anonymous • The potential implications of online abuse • What acceptable and unacceptable online behaviours look like	This risk or harm will be covered in the following curriculum areas: • RSE • Computing • PSHE & Citizenship • Personal Development time including Tutor time sessions and PSHE

Radicalisation	Students are at risk of accessing inappropriate and harmful extremist content online, including terrorist material. Extremist and terrorist groups use social media to identify and target vulnerable individuals. Teaching will include the following: • How to recognise extremist behaviour and content online • Which actions could be identified as criminal activity • Techniques used for persuasion • How to access support from trusted individuals and organisations	All areas of the curriculum
Challenges	Online challenges acquire mass followings and encourage others to take part in what they suggest. Teaching will include the following: • What an online challenge is and that, while some will be fun and harmless, others may be dangerous and even illegal • How to assess if the challenge is safe or potentially harmful, including considering who has generated the challenge and why • That it is okay to say no and to not take part in a challenge • How and where to go for help • The importance of telling an adult about challenges which include threats or secrecy, such as 'chain letter' style challenges	This risk or harm will be covered in the following curriculum areas: • RSE • Personal Development time including Tutor time sessions and PSHE
Content which incites violence	Knowing that violence can be incited online and escalate very quickly into offline violence. Teaching will include the following: • That online content (sometimes gang related) can glamorise the possession of weapons and drugs • That to intentionally encourage or assist in an offence is also a criminal offence • How and where to get help if they are worried about involvement in violence	This risk or harm will be covered in the following curriculum areas: • RSE • Personal Development time including Tutor time sessions and PSHE
Fake profiles	Not everyone online is who they say they are. Teaching will include the following: • That, in some cases, profiles may be people posing as someone they are not or may be 'bots' • How to look out for fake profiles	This risk or harm will be covered in the following curriculum areas: • RSE • Computing • Personal Development

		time including Tutor time sessions and PSHE
Grooming	Knowing about the different types of grooming and motivations for it, e.g. radicalisation, child sexual abuse and exploitation, gangs and financial exploitation. Teaching will include the following: • Boundaries in friendships with peers, in families, and with others • Key indicators of grooming behaviour • The importance of disengaging from contact with suspected grooming and telling a trusted adult • How and where to report grooming both in school and to the police At all stages, it is important to balance teaching students about making sensible decisions to stay safe whilst being clear it is never the fault of the child who is abused and why victim blaming is always wrong.	This risk or harm will be covered in the following curriculum areas: • RSE • Personal Development time including Tutor time sessions and PSHE
Livestreaming	Livestreaming (showing a video of yourself in real-time online, either privately or to a public audience) can be popular with children, but it carries a risk when carrying out and watching it. Teaching will include the following: • What the risks of carrying out livestreaming are, e.g. the potential for people to record livestreams and share the content • That online behaviours should mirror offline behaviours and that this should be considered when making a livestream • That students should not feel pressured to do something online that they would not do offline • The risk of watching videos that are being livestreamed, e.g., there is no way of knowing what will be shown next • The risks of grooming	This risk or harm will be covered in the following curriculum areas: • RSE • Personal Development time including Tutor time sessions and PSHE
Pornography	Knowing that sexually explicit material presents a distorted picture of sexual behaviours. Teaching will include the following: • That pornography is not an accurate portrayal of adult sexual relationships • That viewing pornography can lead to skewed beliefs about sex and, in some circumstances, can normalise violent sexual behaviour	This risk or harm will be covered in the following curriculum areas: • RSE • Personal Development time including

	• That not all people featured in pornographic material are doing so willingly, e.g. revenge porn or people trafficked into sex work	Tutor time sessions and PSHE
Unsafe communication	Knowing different strategies for staying safe when communicating with others, especially people they do not know or have not met. Teaching will include the following: • That communicating safely online and protecting your privacy and data is important, regardless of who you are communicating with • How to identify indicators of risk and unsafe communications • The risks associated with giving out addresses, phone numbers or email addresses to people students do not know, or arranging to meet someone they have not met before • What online consent is and how to develop strategies to confidently say no to both friends and strangers online	This risk or harm will be covered in the following curriculum areas: • RSE • Computing • Personal Development time including Tutor time sessions and PSHE
Wellbeing		
Impact on confidence (including body confidence)	Knowing about the impact of comparisons to 'unrealistic' online images. Teaching will include the following: • The issue of using image filters and digital enhancement • The role of social media influencers, including that they are paid to influence the behaviour of their followers • That 'easy money' lifestyles and offers may be too good to be true • The issue of photo manipulation, including why people do it and how to look out for it	This risk or harm will be covered in the following curriculum areas: • RSE • Personal Development time including Tutor time sessions and PSHE
Impact on quality of life, physical and mental health and relationships	Knowing how to identify when online behaviours stop being fun and begin to create anxiety, including that there needs to be a balance between time spent online and offline. Teaching will include the following: • How to evaluate critically what students are doing online, why they are doing it and for how long (screen time) • How to consider quality vs. quantity of online activity • The need for students to consider if they are actually enjoying being online or just doing it	This risk or harm will be covered in the following curriculum areas: • Health education • Personal Development time including Tutor time sessions and PSHE

	out of habit, due to peer pressure or due to the fear or missing out • That time spent online gives users less time to do other activities, which can lead some users to become physically inactive • The impact that excessive social media usage can have on levels of anxiety, depression and other mental health issues • That isolation and loneliness can affect students and that it is very important for them to discuss their feelings with an adult and seek support • Where to get help	
Online vs. offline behaviours	People can often behave differently online to how they would act face to face. Teaching will include the following: • How and why people can often portray an exaggerated picture of their lives (especially online) and how that can lead to pressure How and why people are unkind or hurtful online when they would not necessarily be unkind to someone face to face	This risk or harm will be covered in the following curriculum areas: • RSE • Personal Development time including Tutor time sessions and PSHE
Reputational damage	What users post can affect future career opportunities and relationships – both positively and negatively. Teaching will include the following: • Strategies for positive use • How to build a professional online profile	This risk or harm will be covered in the following curriculum areas: • RSHE • Personal Development time including Tutor time sessions and PSHE
Suicide, self-harm and eating disorders	Students may raise topics including eating disorders, self-harm and suicide. Teachers must be aware of the risks of encouraging or making these seem a more viable option for students and should take care to avoid giving instructions or methods and avoid using language, videos and images.	

Appendix B **Online Tutoring Protocol and Guidance – Tutor / School**

Introduction

RCT recognises that in some specific circumstances students may need to access their curriculum via 1-to-1 tuition which may need to be provided via an online platform. The following circumstances could apply but this list is not exhaustive, and each case will undergo a due diligence process to ensure that all parties are appropriately safeguarded:

- Student unable to access school due to a medical condition or illness
- Student unable to access school due to SEND related anxiety
- Student unable to access school to significant levels of anxiety
- Students on a plan of phased return to full-time schooling

RCT takes its responsibility seriously for the safety of all those using online platforms to receive, deliver and track education, this can apply whether tutoring is carried out remotely, in school or as part of the National Tutoring Programme (NTP). Students, teachers/tutors, parents/carers, commissioning bodies and RCT personnel are all actively responsible for playing a role in ensuring online safety of both children and adults in the virtual/ remote learning environment, by taking measures to protect them from harm and keeping themselves safe in the broader setting of the virtual world. It is important that all staff who interact with children, including online, continue to look out for signs a child may be at risk. Any such concerns should be dealt with as per the Child Protection and Safeguarding Policy.

Practices set within this protocol must be followed to ensure safety. This applies to all individuals who access RCT systems. It applies to information in all formats, including paper records and electronic data.

Remote working means working off the RCT sites. This includes working while connected to the RCT Wi-Fi networks or the use of personal home networks to access school facilitated tuition.

A mobile device is defined as a portable device which can be used to store or process information. Examples include but are not limited to laptops, tablets, USB sticks, removable disc drives and smartphones.

Other relevant policies and guidance will include: -

- Equality, Equity, Diversity and Inclusion (Staff) Policy
- Equality, Equity, Diversity and Inclusion (Student) Policy
- Child Protection and Safeguarding Policy
- Online Safety Policy
- Working Together to Safeguard Children (2018)
- KCSIE (2024)
- Safer Recruitment Policy
- Data Protection (GDPR) Policy

Online Tutor

An online tutor is there to support and facilitate a learning experience and add extra value to the overall

learning experience.

Online tutors support learners by:

- Responding to students' queries and providing their subject matter expertise
- Initiating learning activities for individuals or groups of students
- Providing feedback to tasks submitted, informally or as part of formal assessment
- Moderating and contributing to online discussions and live chat

All tutors are fully vetted in line with RCT Safer Recruitment Policy.

Roles and Responsibilities:

It is the responsibility of the tutor to ensure that they work securely and protect both data and RCT -owned equipment from loss, damage, or unauthorised access. Tutors are responsible for supporting adherence with this protocol. Additional measures may be put in place by management to ensure the rules contained within this protocol are adhered to (for example monitoring or supervision).

Key Principles of Video Conferencing

When using video conferencing facilities (Microsoft Teams) as part of their day-to-day duties, Tutors must abide by the following: -

- Ensure you have a complex password to access the system: This means having a mixture of numbers, letters, capitals, and possibly special characters.
- Do not share your login credentials with others. No other members of the household should know or can guess your password(s). If passwords are written down (which should be a last case scenario) they must be stored securely (e.g., in a locked drawer or in a secure password protected database/device).
- Passwords should never be left on display for other to see.
- Do not record calls without prior permission (see recordings below for details on when recording is necessary).
- Check all the correct participants are present in the tutoring session: It can be possible for unauthorised users to join video calls. It may be best to start the call with a register if many users are involved on the call.
- Ensure settings are fixed so that other users on the call cannot record the conversation covertly: Check the system's settings to ensure that other users can't record calls. Also remind users at the beginning that they should not record the call.
- External links shouldn't be shared: Video conferencing isn't always encrypted and so can be vulnerable to unauthorised users who can join calls and send links to others (and these links when opened may expose user's account details). At the beginning

of a call, it may be beneficial to remind users not to open any external links sent over chat.

- Sensitive documents shouldn't be shared over video call: Screen share facilities should be used rarely and should contain no personal data where possible. Other users may take a screenshot and then have a copy of data they may not be entitled to.

All messages and interactions by "Chat" facilities should be public

- Preparation/follow up: If you need to send documents or work in advance or following a session, do
- ensure that (1) all users are blind copied (BCC) into the email and (2) to avoid sending any sensitive data (such as health data) in those emails. If you need to send sensitive data to a specific individual, do re-check the email address before sending to check it is being sent to the correct recipient.
- Do not give out personal email addresses and numbers to users. Providing personal details such as phone numbers, social media accounts or email addresses are forbidden in any circumstances. Please ensure you only provide them with official work communications only and email address if provide with one by a school.
- Do report any behavioural or safeguarding concerns to your designated school link immediately.
- Be careful of what is on display in your background. Remove any material which could be construed as inappropriate or offensive. If you are unsure, it is best to blur your background.
- Tutors must ensure they are appropriately dressed to conduct sessions with students
- Students should also be appropriately dressed in day wear.

Key Principles of Virtual Learning and Home Working

In addition to the principles above, it is important to comply with the following principles when conducting virtual learning and home working: -

- To adhere to the principles of the Data Protection Act 2018 and the RCT Acceptable Use Policies.
- Access to personal data must be controlled.
- Portable mobile devices should be encrypted where possible (or at least password/pin code protected) and should never be left unattended in a public place.
- It is the responsibility of each member of staff to ensure that they are working in a safe environment at home. No health and safety risks must be taken when using school equipment. If using personal equipment tutors would be expected to exercise appropriate safe practise. This will also ensure that there is not detrimental impact on the tuition session.
- All personal information and sensitive personal information should be encrypted/password protected before being sent by email where possible. Extra care must be taken when sending emails where auto-complete features are enabled (as this can lead to sending emails to similar/incorrect email addresses).
- Always use your CGS/KSHS/RCT email address when contacting colleagues, students, or parents.

- Any technical problems (including, but not limited to, hardware failures and software errors) which may occur on the systems must be reported to ICT immediately.
- Data should not be stored on personal devices. All data should be saved on RCT systems.
- To be vigilant to phishing emails and not clicking on unsafe links. If clicked these links could lead to malware infection, loss of data or identity theft.
- Users should not access inappropriate websites on RCT devices or whilst accessing RCT networks.
- Students accessing sessions and school resources via personal devices will be expected to comply with acceptable use agreements and other relevant school policies.
- Student/Parents will be advised that using open (unsecured) wireless networks should be avoided. and will be advised to consider configuring devices not to connect automatically to unknown networks.

The Tutor

The Tutor shall:

- Ensure that if no parent/responsible adult is present during a lesson session and the session is being recorded that the student is comfortable to continue the session; if not, they should terminate the session and rearrange when a parent/responsible adult can be present.
- Treat students fairly and without prejudice or discrimination; students who have a disability or come from a minority ethnic or cultural group can easily become victims of discrimination and prejudice which may be harmful to the student's wellbeing.
- Ensure that the tutor environment does not display any inappropriate images or documentation capable of being viewed by the student or parent/responsible adult when conducting a session.
- Ensure that sessions and contact with students only happen between the hours of 8:30 am and 4.30pm Monday to Friday (unless other special arrangements are made)
- Always ensure language is appropriate and not offensive or discriminatory.
- Ensure any contact with the student is appropriate to their role as a tutor and confined to the relevant lesson session.
- Verbal communications in lessons should be appropriate to the lesson content and limited to appropriate professional feedback and comment.

- Where there are concerns that need to be communicated to parents/carers these should be conducted via the designated school link so that they are able to maintain a central overview of provision.
- Value and take students' contributions seriously.
- Continue to look out for signs a child may be at risk and report and such concerns appropriately.
- Report any emergency, dispute or incident with a student or parent/responsible adult to the DSL.

- Report any inappropriate behaviour or illegal activity identified within a lesson session by the student or third party.
- Follow the Key Principals of Video Conferencing contained within this protocol
- Tutors must notify the RCT immediately of a data breach. Any data breach under this scheme must be notified to the evaluators within 48 hours.
- Sessions will be recorded unless individuals have opted out to recordings. The rationale behind recording sessions and how the recordings will be used will be shared with the student and parents/carers to enable them to give informed consent and in accordance with GDPR. If a parent or student indicates they wish to opt out of recording, do let your line link know immediately.
- Check the correct students/parents are invited to the session and that they have agreed to tutoring before sessions begin.
- Student attendance and/or non-attendance must be reported to the line link.
- Any safeguarding concerns must be notified to the DSL.
- Any requests for sessions out of school hours (evenings/weekends) must be approved in advance with your line link to ensure appropriate supervision can be put in place where needed.

The Student

The student shall:

- Ensure that if no parent/responsible adult is present during a lesson session that they are comfortable to continue the session if the session is being recorded; if not, the session will be terminate and rearranged.
- Ensure that sessions and contact with tutors only happens between the hours of 8:30 am and 4:30 pm Monday to Friday (unless other special arrangements are made)
- Treat the tutor with respect and fairness, and not subject them to abusive behaviour or language.
- Have no communication with the tutor outside the lesson session unless this has been agreed as part of the provision and only the school email system is used.
- Report any dispute or incident with a tutor to a parent/responsible adult as soon as possible.
- Report any inappropriate behaviour or illegal activity by a tutor within a session as soon as possible.
- Ensure the tutoring session take place in a public area of the home.
- Ensure they are dressed appropriately in day wear.

School/Parent/Responsible Adult

The school/parent/responsible Adult shall:

- Ensure the student is fully aware of the Acceptable Use (Student) Policy as well as the Child Protection and Safeguarding Policy

- Ensure that if no parent/responsible adult is present during a lesson session that the student understands that if they are comfortable to do so and the session is being recorded, they can opt is to continue the session; if not, session will be rearranged.
- Ensure that sessions and contact with tutors only happens between the hours of 8:30 am and 4:30 pm Monday to Friday (unless other special arrangements are made)
- Always be responsible for the welfare of the student during the session.
- Continue to look out for signs a child may be at risk and report and such concerns appropriately.
- Always be responsible for the physical environment of the student during the session ensuring it is safe and appropriate. If they consider it appropriate, be present or available during a tutor session so any concerns encountered by the student can be reported as soon as possible and ensure the student and tutor are behaving in an appropriate manner.
- Ensure that tutors will be treated with respect and fairness by the student and will not be subjected to abusive behaviour or language.
- Verbal communications in lessons are appropriate to the lesson content and limited to appropriate professional feedback and interaction.
- Ensure the student has no inappropriate communication with the tutor outside the lesson session.
- Report any unsolicited communications between the tutor and student if appropriate.
- Report any inappropriate behaviour or illegal activity identified within a lesson session by the student or third party.

Recordings

RCT protocol is that normal tutoring sessions should be recorded, and agreement should be sought by all parties. Recordings must be saved on RCT systems and should not be transferred onto personal devices. This is to ensure this data is retained in accordance with RCT retention guidelines. Recordings will be secured and disposed of safely in accordance with RCT retention processes.

Shared Online Tuition Sessions

Some online tuition provision takes place with small online groups. Where participants could be from different schools or settings, providers should notify RCT where this might be the case so that the school can ensure that comparable protocols are in place to safeguard its participating students.