The Robert Carre Trust

Online and Digital Safety Policy

Development/Monitoring/Review of this Policy

This online safety policy has been developed through consultation with the following:

- Executive Headteacher/Head of School and senior leadership teams (SLTs) at Trust schools
- Designated Safeguarding Leads (DSL)
- ICT Support Teams
- Social Media School Leads
- Staff – including teachers, support staff, technical staff
- RCT Trust and Local Governing Body Designated Safeguarding Governors
- Student Representatives on Student Council
- Parents and carers

Schedule for Development/Monitoring/Review

This online safety policy was first approved by the Robert Carre Trust on 3 February 2022

The implementation of this online safety policy will be monitored by the:

DSL

SLT

ICT Support Teams

Members of the Online Safety Group

Trust & Local Governing Body Link Governors with Safeguarding responsibilities

Monitoring will take place in line with the agreed schedule of Safeguarding Monitoring visits by designated governor links

Local Governing Bodies will receive a report on the implementation of the online safety policy as part of the agreed schedule for monitoring of safeguarding by designated governor links.

The online safety policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place.

The linked Acceptable Use Policies for students and staff are designed to respond flexibly to concerns and threats with users being informed of any amendments. Acceptance of changes will be automatically secured the next time the user logs in to the network.

Should serious online safeguarding incidents take place, the following persons/agencies should be informed: DSL & Executive Headteacher/Head of School who will assess which relevant authorities (i.e., Children's Services/LADO/Police) should be informed

Should there be serious breaches relating to the digital safety of a Trust school, the following persons will be responsible for determining appropriate action and responses: ICT Support Team; Executive Head Teacher/Head of School

The school will monitor the impact of the policy using:

- Logs of reported incidents
- Monitoring logs of internet activity (including sites visited)/filtering
- Internal monitoring data for network activity
- Consultation with relevant parties (students, staff and parents) as part of the scheduled review process

Scope of the Policy

This policy applies to all members of the Robert Carre Trust community (including staff, students/pupils, volunteers, parents/carers, visitors) who have access to and are users of a Trust school's digital technology systems, both in and out of the school.

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of students when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of online-bullying or other online safety incidents covered by this policy, which may take place outside of the school but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

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

Roles and Responsibilities

The following section outlines the online safety roles and responsibilities of individuals and groups within the Trust schools.

Robert Carre Trust Board & Local Governing Bodies

The RCT Board and Local Governing Bodies are both responsible for reviewing the safeguarding as part of their safeguarding duty. Online safety is part of the annual safeguarding audit carried out by each Trust school which is signed off by each Local Governing Body. Summary reports of the annual audit are available to the RCT Safeguarding link and thus the RCT Board. However, as a Trust policy, final ratification of this policy lies with the Robert Carre Trust Board. The effectiveness of the policy will be monitored as part of the scheduled safeguarding monitoring process.

The Trust and each Local Governing Body have designated members who are responsible for carrying out the scheduled monitoring visits for safeguarding during the course of the year. Monitoring the effectiveness of this policy and associated activities will form part of that monitoring process. Designated governors will draw on the following to inform their monitoring as different stages of the scheduled process:

- Meetings with the DSL at school and school DSLs at Trust level
- Participation in meetings of the online safety group
- Review of monitoring and filtering logs
- The annual safeguarding audit: interim and summary reports

- Executive Headteacher, Head of School and Senior Leaders

The Executive Headteacher/Head of School has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day-to-day responsibility for online safety will be delegated to the DSL and their deputies in each Trust school.

- The Headteacher and DSL should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff. (see Appendix A: flow chart on dealing with online safety incidents Responding to incidents of misuse)
- Ensure that staff access appropriate training as part of the school's CPD offer
- Training needs will be assessed by the school DSLs who, in consultation with CPD leads, will identify appropriate online platforms and other providers to support staff in carrying out their safeguarding responsibilities with regard to online and digital safety. Records of staff training are maintained by the DSL and CPD leads)
- Executive Headteacher/Head of School and Senior Leaders will ensure that there is an effective monitoring and filtering system in place that facilitates safe access to online and digital technology for all users. They will also be cognisant of the support needs of staff who are involved in monitoring activity.
- The Robert Carre Trust schools use the following monitoring and filtering system: SENSO
- The Senior Leadership Team and DSL will have access to regular SENSO monitoring reports but the DSLs and their deputies will lead on the school response to any safeguarding alerts

Designated Safeguarding Lead (Online Safety Lead)

In Trust schools the DSL will fulfil the role of Online Safety Lead supported by their deputies and the wider safeguarding team, ICT Services Manager and the ICT teams. They will:

- be trained in online safety issues and be aware of the potential for serious child protection/safeguarding issues to arise from:
    - sharing of personal data
    - access to illegal/inappropriate materials
    - inappropriate on-line contact with adults/strangers
    - potential or actual incidents of grooming
    - online-bullying

The Trust recognises that these are safeguarding rather than technical issues but, that the technology provides an environment and means where significant safeguarding issues could develop.

- Monitor the effectiveness of the systems in place to safeguard students engaged in online and/or digital activity
- takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies/documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- Oversee the investigation and management of online safety incidents, delegating to the relevant Head of Year where appropriate
- Oversee the provision of training and advice for staff and liaise with CPD leads in the planning and provision of safeguarding training.

- Liaise with appropriate external bodies such as the Local Authority, Police, Children's Services
- liaise with the ICT Support Team
- Receive and respond to reports of online safety incidents and monitor the log of incidents in Bromcom which will also inform future online safety developments,
- meet regularly with the designated Local Governing Body safeguarding governors to discuss current issues, review incident logs and filtering/change control logs as part of the scheduled monitoring process for safeguarding. Mechanisms are in place to ensure that appropriate feedback is provided to the Trust Board.
- Participate in relevant meetings of the online safety group, the Trust or Local Governing Body to review the effectiveness of the policy
- report regularly to Senior Leadership Team

ICT Services Manager and ICT Support Team

Those with technical responsibilities in Trust Schools are responsible for ensuring:

- that the school technical infrastructure is secure and is not open to misuse or malicious attack
- that the school meets required online safety technical requirements and any Local Authority/MAT/other relevant body online safety policy/guidance that may apply.
- that users may only access the networks and devices through a properly enforced password protection policy
- the filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person (see Appendix B: Technical Security Protocols for good practice)
- that they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- that the use of the networks/internet/digital technologies is regularly monitored in order that any misuse/attempted misuse can be reported to the Executive Headteacher/Head of School, DSL and Head of Year for investigation/action/sanction
- that monitoring software/systems are implemented and updated as agreed in Trust and School policies
- The ICT Services Manager will advise CPD leads with regard to staff training in digital and online safety so that CPD leads can maintain an overview of staff training provision and ensure that all relevant staff have access to both time and hardware to complete the training.

All Staff

Are responsible for ensuring that:

- they have an up-to-date awareness of online safety matters and of the current Trust online safety policy and practices
- they have read, understood and signed the staff Acceptable Use Policy (AUP) (See link in Appendix C)
- Recognise that the AUP can be amended during the course of an academic year to respond to safety concerns and that each time they log on to the school network they are agreeing to any such amendments that they have been notified of
- they report any suspected misuse or problem to the Executive Headteacher/Head of School/DSL(for investigation/action/sanction
- all digital communications with students/parents/carers should be on a professional level and only carried out using official school or school approved systems

- they are aware of the Curriculum Principles for Online and Digital Safety outlined in Appendix B
- students/pupils understand and follow the Online Safety Policy and acceptable use policies
- they act as good role models in their use of digital technologies, the internet and mobile devices they monitor the use of digital technologies, mobile devices, cameras, etc. in lessons and other school activities (where allowed) and implement current policies with regard to these devices

The Online Safety Team

The Online Safety Team in a Trust school draws on various members of staff who have relevant expertise or who represent key user groups: the DSL, SLT Pastoral link, ICT Services Manager, Heads of Year, ICT Teachers, PSHE Coordinator, Social Media Lead, LGB link governor and parent governors. Students will be represented through the school council. This group will play a key role in the consultation and review process regarding online safety and the Online Safety Policy including the impact of initiatives.

The DSL will lead on the policy review process but will consult members of the online safety team where required to ensure the policy is both appropriate and effective. The school's meeting protocols ensure that all members of this team have the opportunity to feed into the review process throughout the year but, where deemed necessary, the DSL can convene a meeting of relevant parties to ensure the annual review is robust.

Students:

- are responsible for using the school digital technology systems in accordance with the student acceptable use policy (see link in Appendix C)
- Recognise that the AUP can be amended during the course of an academic year to respond to safety concerns and that each time they log on to the school network they are agreeing to any such amendments that they have been notified of
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking/use of images and on online-bullying.
- should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's online safety policy covers their actions out of school, if related to their membership of the school

Parents/carers

Parents/carers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way. Trust schools will take every opportunity to help parents understand these issues through a variety of media: newsletters, letters, website, social media and information about national/local online safety campaigns/literature. Parents and carers will be encouraged to support the school in promoting good online safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- access to parents' sections of the website and on-line student records

- their children's personal devices in the school as outlined in the use of mobile phones protocols (see Appendix C)

Community Users

Community Users who access school/academy systems or programmes as part of the wider school/academy provision will be expected to sign the staff or student AUP (whichever is appropriate) before being provided with access to school/academy systems.

Policy Statements

Education – Students/Pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating students to take a responsible approach. The education of students in online safety/digital literacy is therefore an essential part of a Trust school's online safety provision. Children and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience.

In planning their online safety curriculum Trust Schools will draw upon:

- KCSIE: Annex D Online Safety – Information and Support
- DfE Teaching Online Safety in Schools
- Education for a Connected Word Framework
- The AUP for students (see link in Appendix C)
- Any trending concerns identified by monitoring logs or feedback from the online safety team
- Local online safety concerns

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- Online and digital safety are part of the ICT curriculum at KS3
- The Curriculum Online and Digital Safety Principles will apply to all learning activities (See Appendix B)
- Key online safety messages are reinforced as part of the planned PSHE programme through assemblies and tutorial/pastoral activities
- It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g., racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the ICT Support Team temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.
- Students/pupils should be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making.

Education – Parents/carers

Many parents and carers may only have a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring/regulation of their children's online behaviours. Parents may underestimate how

often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The school/academy will therefore seek to provide information and awareness to parents and carers through:

- Curriculum activities
- Letters, newsletters, web site, social media
- Year Group Information Evenings for Parents
- High profile events/campaigns e.g., Safer Internet Day
- Signposts to relevant web sites/publications via the website

The Trust would recommend the Think U Know website as a source of information for parents as it is the website linked to the government agency at the frontline of online safety: CEOP (Child Exploitation and Online Safety). The website allows parents to filter the guidance available according for the following age groups: 4-7. 8-10. 11-13 and 14+. (See Appendix D for weblink)

Education – The Wider Community & Outreach Activities

Trust schools supports local primary schools in the delivery of some areas of their curriculum, currently PE and Science, and remains committed to supporting the wider educational community with our expertise and facilities. Where the delivery of these areas of the curriculum involve access to digital or online resources Trust staff will be cognisant of the opportunity to educate the pupils in safe practice.

The Trust recognises that students are members of families and the wider community and take part in community activities. Online safety messages and signposting will take into account these wider community links.

Trust schools will also be open to sharing their online safety expertise and practice with other local schools and community groups.

Education & Training – Staff/Volunteers

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

- The DSL and Online Safety Team will receive regular updates through attendance at relevant safeguarding briefings, training or webinars and by reviewing guidance documents released by relevant organisations.
- The DSL and ICT Services Manager will liaise with CPD leads to ensure that online and digital safety training is available to staff as part of the annual safeguarding training
- Training needs will be reviewed as part of the policy review process and where required, will be responsive to any serious online incident
- Where online or digital safety incidents suggest members of staff would benefit from targeted training this will be facilitated
- All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the Trust online safety policy, AUPs and Curriculum Principles for Online and Digital safety
- The DSL will provide advice/guidance/training to individuals as required.

Training – Governors

Governors should take part in online safety training/awareness sessions, with particular importance for those who are members of any group involved in technology/online safety/health and safety /safeguarding. This may be offered in a number of ways:

- Attendance at training or webinars provided by a relevant organisation or online platform
- Participation in school training/information sessions for students, staff or parents, This may include attendance at assemblies/lessons by the relevant link governors for online safety and safeguarding

Technical – infrastructure/equipment, filtering and monitoring

A Trust school will be responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their online safety responsibilities:

Technical Security

- School technical systems will be managed in ways that ensure that the school meets recommended technical requirements
- There will be regular reviews and audits of the safety and security of school technical systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to school technical systems and devices.
- All users will be provided with a username and secure password by ICT Support who maintain an up-to-date record of users and their usernames. Users are responsible for the security of their username and password.
- The “master/administrator” passwords for the school systems, used by the ICT Services Manager (or other members of ICT Support) must also be available to the Executive Headteacher/Head of School or other nominated senior leader and kept in a secure place
- The ICT Services Manager is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations. .
- Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. There is a clear process in place to deal with requests for filtering changes.
- Internet filtering/monitoring is cognisant of our responsibilities under the terms of the Prevent Duty to safeguard students from radicalisation
- The school has provided enhanced/differentiated user-level filtering allowing different filtering levels for different groups of users – staff/students
- Trust schools use SENSO cloud for filtering and monitoring purposes which includes their remote monitoring service. The service protects users using school-owned devices whether they are in school or learning from home, by proactively monitoring and indicating to relevant staff, users who may be vulnerable or at risk, users who may pose a risk to others and inappropriate, off-task or harmful behaviour.

- Users should report any actual/potential technical incident/security breach to ICT Support; where breachers raise safeguarding concerns these will be reported to the DSL
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, workstations, mobile devices, etc. from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual devices are protected by up-to-date virus software.
- The provision of temporary access of "guests" (e.g. trainee teachers, supply teachers, visitors) onto the school systems is managed through ICT Support and is restricted to appropriate access levels.
- The AUP includes the extent of personal use that users (staff/students) and their family members are allowed on school devices that may be used out of school.
- The AUP outlines the protocols for downloading executable files and installing programmes on school devices.
- The AUP outlines the protocols for the use of removable media (e.g. memory sticks/CDs/DVDs) by users on school devices. Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

Mobile Technologies including RCT Bring Your Own Device Policy (BYOD)

Mobile technology devices may be school owned/provided or personally owned and might include: smartphone, tablet, notebook/laptop or other technology that usually has the capability of utilising the school's wireless network. The device then has access to the wider internet which may include the school's learning platform and other cloud-based services such as email and data storage.

All users should understand that the primary purpose of the use of mobile/personal devices in a school context should be educational.

Use of own devices is covered by the BYOD Policy available on the RCT website policies section.

Mobile Phone use by students is detailed in the relevant Mobile Phone Policy on each school website.

Both policies are inter-related to other relevant policies including but not limited to: AUPs, Safeguarding, Behaviour, Anti-Bullying and the Online and Digital Safety Policy.

The links to the relevant polices and AUPs can be found in Appendix C.

BYOD & Access to the school Network is detailed in the relevant AUP (see link in Appendix C)

School owned/provided devices and accessories will take into account the following considerations:

- They will be allocated to students based on identified or assessed need and will remain school property
- Devices configured for home use will not be able to access the school systems in school
- The primary purpose of devices configured for home use is to support education in the home setting
- Devices configured for use in school will not be usable at home
- Users of all such devices will be subject to the relevant AUP (see Appendix C) and the principles outlines in this policy
- School owned devices will be monitored for appropriate use and users can be required to submit a device for monitoring purposes when requested

- ICT Support will provide technical support for the device but not for access to personal networks or peripherals

Personal Devices, and Visitor AUP

- Where required to facilitate the delivery of their sessions, external visitors will have guest access to the network with appropriate restrictions activated for their devices.
- Technical support will only be available for issues relating to the school network and not personal devices or accessories
- The visitor is responsible for their equipment complying with health and safety requirements; if personal equipment is not deemed to comply with these requirements the school reserves the right to decline access to the school network
- Visitors should ensure that students are not exposed to inappropriate personal content on the visitor's device
- Visitors should be aware that exposing students to inappropriate content or accessing inappropriate content while using the school network would be reported to the school's designated safeguarding lead
- Visitors should not allow students to access their devices
- Visitor devices should not be left unattended and unlocked
- The school cannot be held liable for damage or loss where devices are left unattended and/or insecure
- Guest users will be made aware of these protocols for visitor use

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents/carers and students need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for online-bullying to take place. Some may actually be illegal images if they feature minors under the age of 18 and are deemed to be sexual in nature. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate students about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g., on social networking sites.
- Written permission from parents or carers is obtained on entry to the school and will determine if photographs of students are published on the school website/social media/local press
- In accordance with guidance from the Information Commissioner's Office, parents/carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published/made publicly available on social networking sites, nor should parents/carers comment on any activities involving other students in the digital/video images.
- Staff and volunteers are allowed to take digital/video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment; the personal equipment of staff should not be used for such purposes.

- Care should be taken when taking digital/video images that students are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Students must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include students will be selected carefully and will comply with good practice guidance on the use of such images.
- Students' full names will not be used in relation to photographs anywhere on a website or blog; full names may be used where no photograph is featured
- Students' work can only be published with the permission of the student; staff should have oversight of online student blogs or articles to ensure that students are not disclosing information that could risk harm to themselves or others

Data Protection

Personal data will be recorded, processed, transferred and made available according to the current data protection legislation and the RCT GDPR Policy (see link to policy in Appendix C).

The Robert Carre Trust ensures that:

- it implements the data protection principles and is able to demonstrate that it does so through use of policies, notices and records.
- it has paid the appropriate fee Information Commissioner's Office (ICO) and included details of the Data Protection Officer (DPO).
- it has appointed an appropriate Data Protection Officer (DPO) who has a high level of understanding of data protection law and is free from any conflict of interest.
- Trust schools also employ a Data Manager to ensure compliance with GDPR and to support the DPO

Staff must ensure that they:

- at all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse
- can recognise a possible breach, understand the need for urgency and know who to report it to within the school
- can help data subjects understands their rights and know how to handle a request whether verbal or written. Know who to pass it to in the school
- will not transfer any school/academy personal data to personal devices (including USBs) except as in line with school policy; USB devices should be encrypted and password protected
- access personal data sources and records only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data
- computers will not be left unlocked and unattended

Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the school currently considers the benefit of using these technologies for education outweighs their risks/disadvantages: (*see Table p12*)

	Staff & other adults				*Student*			
Communication Technologies	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to the school								
Use of mobile phones in lessons (Personal use)								
Use of mobile phones (educational use /Authenticator)								
Use of mobile phones in social time							SEN	
Taking photos on personal devices (People in lessons)								
Taking photos on personal devices (Objects work related)								
Taking photos on personal devices (social time)								
Use of other mobile devices e.g. tablets, laptops								
Use of personal email addresses in school or on school network								
Use of school/academy email for personal emails								
Use of messaging apps								
Use of social media								
Use of blogs								

When using communication technologies, the school/academy considers the following as good practice:

- The official school email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored. Staff and students/pupils should therefore use only the school email service to communicate with others when in school, or on school systems (e.g., by remote access).
- Users must immediately report, to the relevant person, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication. Students should report to their teacher or a member of staff; Staff should report to their line manager or the DSL.
- Any digital communication between staff and students or parents/carers (email, social media, chat, blogs, VLE etc) must be professional in tone and content. These

communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or social media must not be used for these communications.
- When emailing the same email to multiple recipients bcc should be used to protect the privacy of recipients
- Students should be taught about online safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

Social Media - Protecting Professional Identity

All schools and MATs have a duty of care to provide a safe learning environment for pupils and staff. Schools and MATs could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, engage in online bullying, discriminate on the grounds of sex, race or disability or who defame a third party may render the school or MAT liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school through:

- Ensuring that personal information is not published
- Training is provided including: acceptable use; social media risks; checking of settings; data protection; reporting issues.
- Clear reporting guidance, including responsibilities, procedures and sanctions
- Risk assessment, including legal risk

School/academy staff should ensure that:

- No reference should be made in social media to students, parents/carers or school staff
- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to the school or MAT
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information

When official school social media accounts are established there should be:

- A process for approval by senior leaders
- Clear processes for the administration and monitoring of these accounts – involving at least two members of staff
- A code of behaviour for users of the accounts, including
    - Systems for reporting and dealing with abuse and misuse
    - Understanding of how incidents may be dealt with under school disciplinary procedures

Personal Use:

- Personal communications are those made via a personal social media accounts. In all cases, where a personal account is used which associates itself with the school/or impacts on the school, it must be made clear that the member of staff is not

communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy
- Personal communications which do not refer to or impact upon the school are outside the scope of this policy
- Where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken
- The school permits reasonable and appropriate access to private social media sites

Monitoring of Public Social Media:

- As part of active social media engagement, it is considered good practice to pro-actively monitor the Internet for public postings about the school
- The school should effectively respond to social media comments made by others according to a defined policy or process

The school's use of social media for professional purposes will be monitored and reviewed to ensure compliance with the school policies and values.

Dealing with unsuitable/inappropriate activities

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned from school and all other technical systems. Staff accessing such material would face disciplinary action, which could result in dismissal and the matter being referred to the appropriate authorities. Other activities e.g. cyber-bullying are banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would be inappropriate in a school context, either because of the age of the users or the nature of those activities.

The Trust believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in/or outside the school when using school equipment or systems. The school policy restricts usage as follows: see Table p15

User Actions	Acceptable	Acceptable at certain	Acceptable for nominated	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:					
Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978					
Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					
Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					
Criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986					
Pornography					
Promotion of any kind of discrimination					
Threatening behaviour, including promotion of physical violence or mental harm					
Promotion of extremism or terrorism					
Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute					

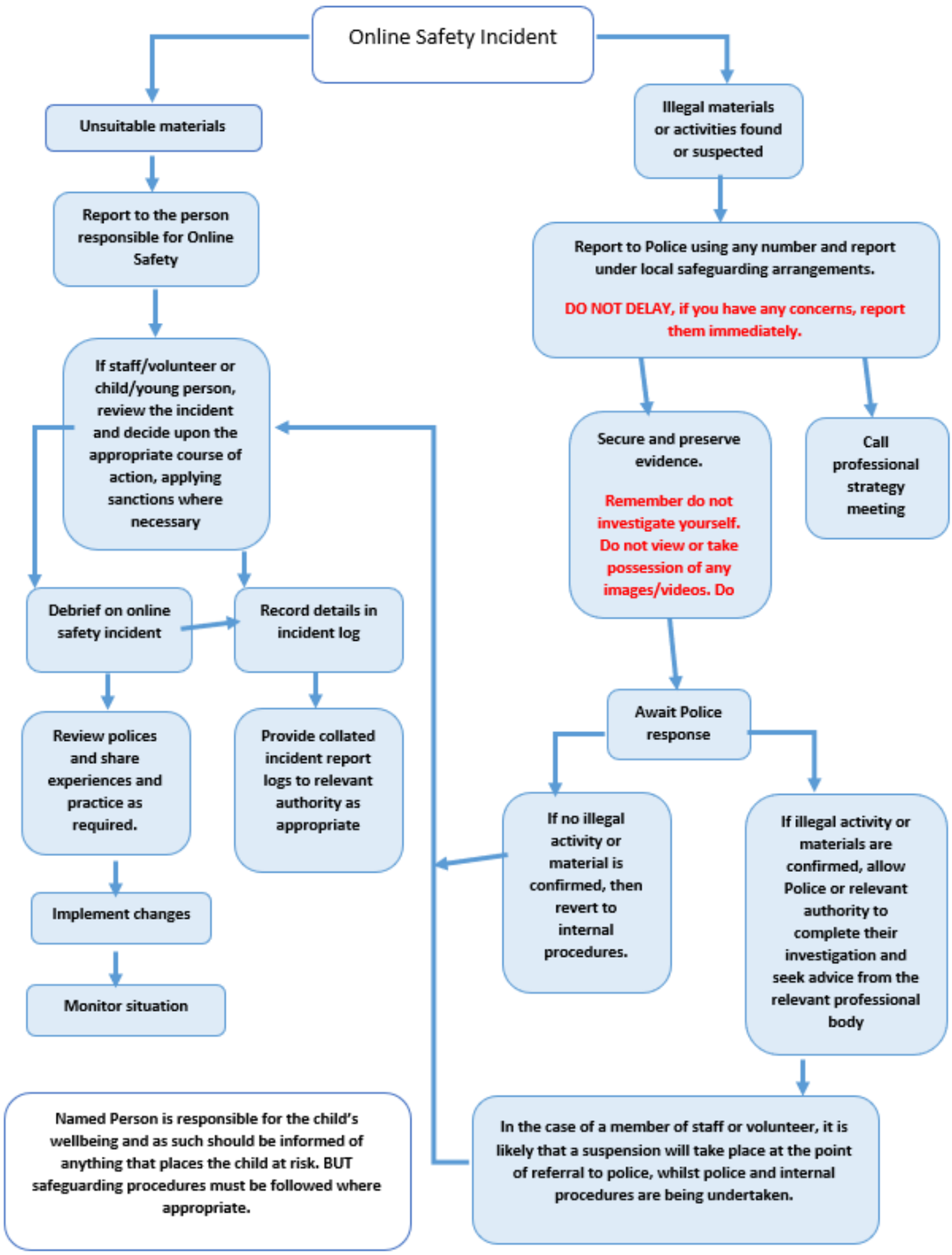
Responding to incidents of misuse

This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities (see “User Actions” above). *See Table p16*

User Actions	Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Activities that might be classed as cyber-crime under the Computer Misuse Act: • Gaining unauthorised access to school networks, data and files, through the use of computers/devices • Creating or propagating computer viruses or other harmful files • Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords) • Disable/Impair/Disrupt network functionality through the use of computers/devices • Using penetration testing equipment (without relevant permission) For serious or repeat offences the Trust reserves the right to report the matter to the police.					
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school/academy					
Revealing or publicising confidential or proprietary information (e.g. financial/personal information, databases, computer/network access codes and passwords)					
Unfair usage (downloading/uploading large files that hinders others in their use of the internet)					
Using school systems to run a private business					
Infringing copyright					
On-line gaming (educational)					
On-line gaming (non-educational)					
On-line gambling					
On-line shopping/commerce					
File sharing					
Use of social media (Staff Personal devices)					
Use of messaging apps (Staff Personal devices)					
Use of video broadcasting e.g., Youtube (Staff use only)					

Illegal Incidents

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right-hand side of the Flowchart (below and appendix) for responding to online safety incidents and report immediately to the police.



Other Incidents

It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow school policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

In the event of suspicion, all steps in this procedure should be followed:

- Have more than one senior member of staff involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the student's record (except in the case of images of child sexual abuse – see below). The incident should be logged in Bromcom.
- Once this has been completed and fully investigated the DSL and SLT will need to judge whether this concern has substance or not. If it does, then appropriate action will be required and could include the following:
    - Internal response or discipline procedures
    - Involvement by Local Authority/Academy Group or national/local organisation (as relevant).
    - Police involvement and/or action
- If content being reviewed includes images of child abuse, then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:
    - incidents of 'grooming' behaviour
    - the sending of obscene materials to a child
    - adult material which potentially breaches the Obscene Publications Act
    - criminally racist material
    - promotion of terrorism or extremism
    - offences under the Computer Misuse Act (see User Actions chart above)
    - other criminal conduct, activity or materials
- Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.

It is important that all of the above steps are taken as they will provide an evidence trail for the school and possibly the police and demonstrate that visits to these sites were carried out for safeguarding purposes. The completed form should be retained by the group for evidence and reference purposes.

School actions & sanctions

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through the normal

Behaviour procedures. The table below details the levels of consequence that could be applied for different breaches.

Level of Consequence	Details
Advice /Guidance (A&G)	Inadvertent or misguided misuse
Internal Sanctions	Breach of AUP/Mobile Device Policy: Misuse of resources; Inappropriate search/content accessed; Sharing / offensive content (including bullying/harassment);
Off-site Sanctions	Abusive /Targeted Against Individual; Significant / Repeated Breaches of AUP/ System Security
External Sanctions	Serious Breaches of AUP/ System Security; Illegal Activity including Plagiarism
Repeated breachers or multiple breaches in one incident could incur escalating / more serious consequences	
Where the misuse is related to home activity parents would be informed for parental action	

Students Incidents (not exhaustive) *Each case is always considered individually with due consideration for mitigating factors such as SEND. Persistent offences will incur more serious consequences.*	Parent Meeting	A&G	Internal	Off-site	External
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable/inappropriate activities).					
Unauthorised use of non-educational sites during lessons					
Unauthorised/inappropriate use of mobile phone/ other device					
Unauthorised/inappropriate use of social media/ messaging apps/personal email					
Unauthorised downloading or uploading of files					
Allowing others to access school network by sharing username and passwords					
Attempting to access or accessing the school network, using another student's/pupil's account					
Attempting to access or accessing the school network, using the account of a member of staff					
Corrupting or destroying the data of other users					
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature					
Continued infringements of the above, following previous warnings or sanctions					
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school					
Using proxy sites or other means to subvert the school's filtering system					
Accidentally accessing offensive or pornographic material and failing to report the incident					
Deliberately accessing or trying to access offensive or pornographic material					
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act					

Staff Incidents

Actions / Sanctions

Staff Incidents *This table is only indicative of potential consequences and it may not cover every policy breach that could occur.* *Incidents that involve a combination of misuse or inappropriate conduct may attract more severe actions*	Refer to line manager	Refer to Headteacher Principal	Refer to LADO	Refer to Police	Refer to Technical Support Staff for action re filtering etc	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable/inappropriate activities).								
Inappropriate personal use of the internet/social media/personal email								
Unauthorised downloading or uploading of files								
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account								
Careless use of personal data e.g. holding or transferring data in an insecure manner								
Deliberate actions to breach data protection or network security rules								
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software								
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature								
Using personal email/social networking/instant messaging/text messaging to carrying out digital communications with students/pupils								
Actions which could compromise the staff member's professional standing								
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school/academy								
Using proxy sites or other means to subvert the school's filtering system								
Accidentally accessing offensive or pornographic material and failing to report the incident								
Deliberately accessing or trying to access offensive or pornographic material								
Breaching copyright or licensing regulations								
Continued infringements of the above, following previous warnings or sanctions								

Appendices

A Flowchart of Incident Response Actions

B Curriculum Principles for Online and Digital Safety

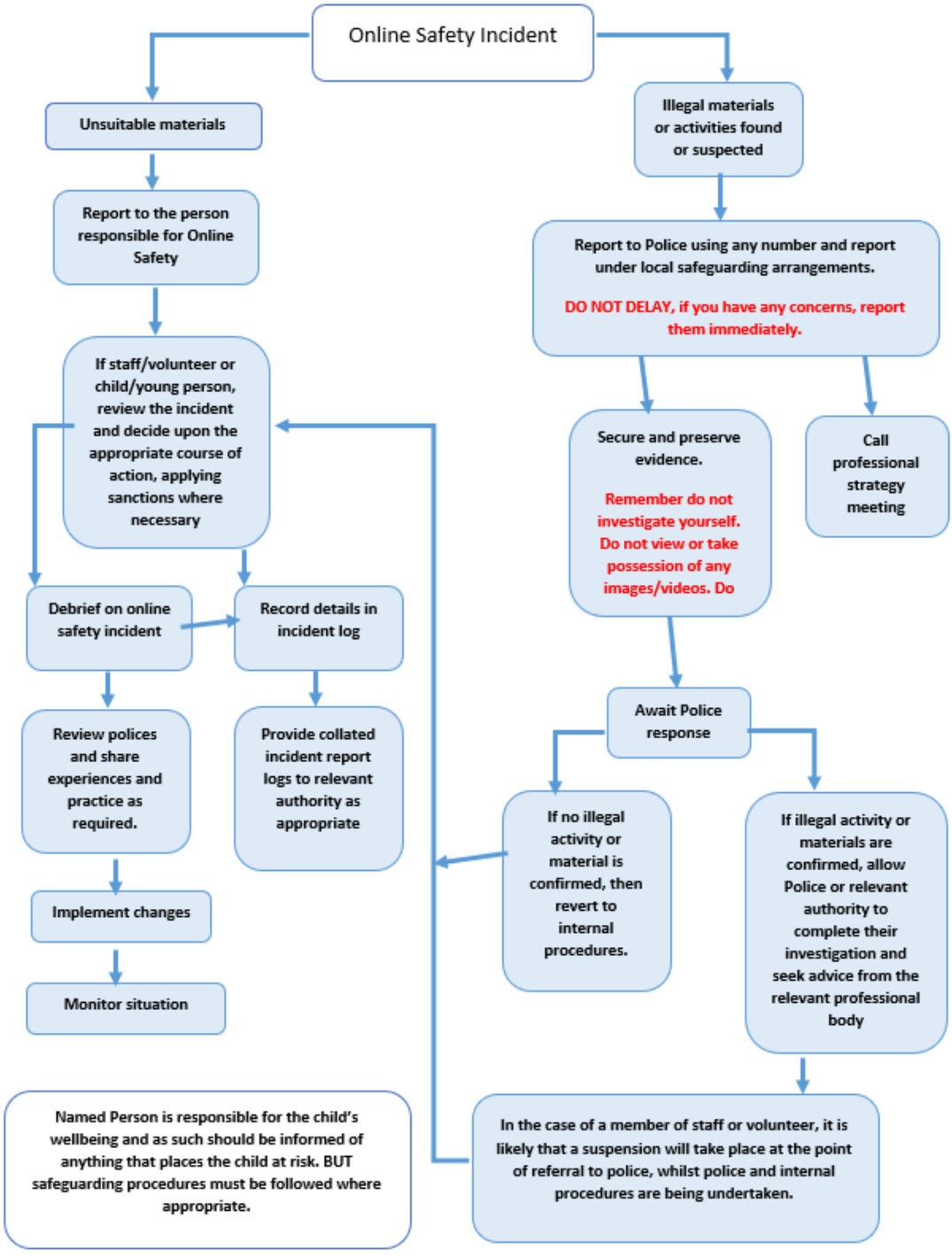
C Links to policies associated with online and digital safety:

D Visitor AUP

Adopted at the meeting of the Board on 3 February 2022

Next Review Date: February 2023 (Annually)

Appendix A Flowchart Of Incident Response Actions



Appendix B Curriculum Principles for Online & Digital Safety

The Robert Carre Trust defines the curriculum as constituting any subject or PSHE programme delivered to students as part of their scheduled provision. However, pastoral interactions and what is sometimes referred to as the "hidden curriculum" will also provide school staff with opportunities to inculcate the principles outlined below. School staff will draw on the framework outlined in the document Education for a Connected World (2020) to determine what is age-appropriate.
(https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/896323/UKCIS_Education_for_a_Connected_World_.pdf)

The Trust deems safety to cover safeguarding academic potential and integrity as well as personal online safety.

The Trust recognises that the use of information and computer technology is now an integral part of our 21st century society and the world of work. It also accepts that access to online resources enriches the delivery of the curriculum and equips the students with skills they can take forward into further education and the world of work. However, it also acknowledges that misuse of these resources, whether intentional or incidental, can result in significant harm to both the students themselves and others. Trust schools are therefore committed to reinforcing and emphasising the principles of safe and respectful practice detailed below in their delivery of education.

- Students will be expected to agree to an acceptable use policy (AUP) in order to access online resources and ICT equipment in school
- Teachers will endeavour to remind students of the relevant aspects of the AUP to reinforce appropriate conduct when incorporating ICT and network resources in the delivery of a topic or part of a topic
- Students will face consequences for any breach of the agreement which may include a deprivation of independent access to the school network and associated resources
- Students without independent access will be able to access the network and resources at the explicit request of a subject teacher who will closely supervise access during their lesson
- When using computers to produce or support the production of work teachers will:
    - Ensure students understand how to conduct appropriate internet searches
    - Encourage students to report any inappropriate results from a search they have instigated to an appropriate adult (ie a teacher in school or a parent/carer at home)
    - Ensure students understand the misuses of information and/or resources that could constitute plagiarism
    - Remind students that copying another student's work or collaboration with other third parties constitute plagiarism if they seek to pass their work off as their own work
    - Instruct students of the academic protocols they should follow when citing someone else's work

- With regard to internet searches, Trust school staff will ensure that:
    - in lessons where internet use is pre-planned students should be guided to sites checked as suitable for their use and be aware of the processes in place for dealing with any unsuitable material that is found in internet searches
    - Where students are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.

    - Students know that searches are monitored, and use of inappropriate words or searches may trigger a safeguarding alert and/or a disciplinary consequence
    - Students understand that searches involving aspects or proponents of terrorism will trigger a concern under the PREVENT strategy and could result in a referral to external agencies
    - Students understand that searches that relate to illegal activity could trigger police involvement
    - Students understand how to assess the reliability and authority of information found as a result of searches
    - Students understand that internet search engines use algorithms to direct enquirers to similar sources of information and that they may need to enter a different search string to achieve a balance of opinion
    - Students develop a growing understanding of the principles and process of academic validation by one's academic peers
    - Students know that if they are concerned by anything that they encounter online they should talk to a parent/carer or member of staff
- Students will be made aware of the potential negative impact of pornography on intimate relationships and that accessing such material could return images that are illegal
- Students will be made aware of the risks associated with social media and other online platforms and media such as:
    - Over-sharing of personal information
    - Safeguarding their online identity
    - Assessing the identity of people seeking to connect online
    - Grooming for sexual or criminal exploitation
    - Self-generated sexual images and the potential consequences
    - Peer on peer abuse and online bullying
    - The legal consequences of inappropriate or illegal activity
- Students will be signposted to appropriate support if they have been the victims of harm as a result of online activity
- Students will also be sign-posted to relevant online resources that support positive mental wellbeing
- School staff will consider the impact on language acquisition of students relying entirely on grammar and spell-checking tools (SPAG Tools) which will not be available in formal assessments and examinations; students could be encouraged to deselect SPAG tools until they have attempted to proof check for themselves
- Students with learning difficulties will be supported in the appropriate and effective use of ICT to support their learning.

Appendix C: Links to associated policies

Current versions of Trust and School policies can be accessed on the websites:

Robert Carre Trust - Policies

Carre's Grammar School - Policies (carres.uk)

Kesteven & Sleaford High School - Policies (kshs.uk)

RCT GDPR Policy

RCT ICT - Acceptable Use (Staff) Policy

RCT ICT - AUP & Media Forms

RCT ICT – Bring Your Own Device (BYOD)

RCT Safeguarding (Child Protection) Policy

RCT Social Media Policy

CGS Behaviour Management Policy

CGS Mobile Phone and Device Policy

KSHS Behaviour Policy

KSHS Mobile Phone and Device Policy

Appendix D AUP for Visitors

- Where required to facilitate the delivery of their sessions, external visitors will have guest access to the network with appropriate restrictions activated for their devices.
- Technical support will only be available for issues relating to the school network and not personal devices or accessories
- The visitor is responsible for their equipment complying with health and safety requirements; if personal equipment is not deemed to comply with these requirements the school reserves the right to decline access to the school network
- Visitors should ensure that students are not exposed to inappropriate personal content on the visitor's device
- Visitors should be aware that exposing students to inappropriate content or accessing inappropriate content while using the school network would be reported to the school's designated safeguarding lead
- Visitors should not allow students to access their devices
- Visitor devices should not be left unattended and unlocked
- Visitors must accept that the school cannot be held liable for damage or loss where devices are left unattended and/or insecure
- Guest users will be made aware of these protocols for visitor use