THE CARLTON INFANT ACADEMY™

REDHILL ACADEMY TRUST
Equality and Achievement

Online Safety Policy

Including: Mobile Technologies, Academy Technical Security and Acceptable Use Policies

Written in accordance with the

Social Media Policy

December 2023

Review: December 2025

Online Safety Lead – Nicole Lang

Signed: Anna Scrivens (Headteacher)

Signed: Rachel Horton

What is this Policy?

Online safety is an integral part of safeguarding and requires a whole academy, cross-curricular approach and collaboration between key academy leads. Accordingly, this policy is written in line with 'Keeping Children Safe in Education' 2023 (KCSIE), 'Teaching Online Safety in Academies', statutory RSHE guidance and other statutory documents. It is cross-curricular (with relevance beyond Relationships, Health and Sex Education, Citizenship and Computing) and designed to sit alongside or be integrated into school's statutory Child Protection & Safeguarding Policy. Any issues and concerns with online safety must always follow the academy's safeguarding and child protection procedures.

Development/Monitoring/Review of this Policy

This policy is a living document, subject to a full annual review but also amended where necessary during the year in response to developments in the academy and local area.

This Online Safety Policy has been developed by:

- Headteacher/Senior Leaders
- Online Safety Lead
- Staff – including Teachers, Support Staff, Technical staff
- Governors
- Parents and Carers
- Pupils

Schedule for Development/Monitoring/Review

The implementation of this Online Safety Policy will be monitored by the: Headteacher: Anna Scrivens Safeguarding Governor: Claire Whiteside	
The Governing Body will receive a report on the implementation of the Online Safety Policy (which will include anonymous details of online safety incidents) at regular intervals:	Annually: September
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 next anticipated review date will be:	Annually: September
Should serious online safety incidents take place, the following should be informed: Headteacher (DSL) or in her absence, Deputy DSL, Online Safety Lead, Chair of Governors, Safeguarding Lead, LADO or the Police	

The academy will monitor the impact of the policy using:

- Logs of reported incidents
- Filtering of Broadband
- Monitoring by SENSO Alerting Software
- Pupil Voice
- Monitoring of planning and pupil's work

Who is in charge of online safety?

KCSIE makes clear that "the designated safeguarding lead, Anna Scrivens should take **lead** responsibility for safeguarding and child protection (including online safety)." The DSL can delegate activities but not the responsibility for this area.

How will this policy be communicated?

This policy will be accessible to and understood by all stakeholders. It will be communicated in the following ways:

- Posted on the academy website
- Part of academy induction for all new staff (including temporary, supply and non-classroom-based staff and those starting mid-year)
- Integral to safeguarding updates and training for all staff (especially in September refreshers)
- Clearly reflected in the Acceptable Use Policies (AUPs) for staff, volunteers, contractors, governors, pupils and parents/carers
- Acceptable Use Policy for parents/carers and pupils are shared via the school website and paper copies are available upon request
- Acceptable Use Policy discussed with pupils and agreed to at the start of the year
- Acceptable Use Policies for all adults who are in the academy are signed and held in the office

Handling Complaints

The academy will take all reasonable precautions to ensure that people are safe online. However, owing to the international scale and linked nature of internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on an academy computer or mobile device. Staff and pupils are given information about infringements in use and possible sanctions. Sanctions available include:

1. Discussion with the Headteacher.
2. Informing parents or carers.
3. Removal of internet or computer access for a period.
4. Referral to the Police.

Any complaint about pupil misuse should initially be reported to the class teacher who then reports it to the Headteacher or Online Safety Lead.
Any complaint about staff misuse is referred to the Headteacher and/or the Chair of Governors.
Complaints of online bullying are dealt with in accordance with our Anti-Bullying Policy.
Complaints related to child protection are dealt with in accordance with the academy's child protection procedures.

Current Online Safeguarding Trends

Over the past year, we have particularly noticed the following in terms of device use and abuse and types of online/device-based incidents which affect the wellbeing and safeguarding of our pupils:

- The use of YouTube and watching inappropriate content which leads to anxiety and confusion over what has been seen.
- The use of TikTok and the algorithm it uses to steer pupils towards looking at inappropriate links such as body image.

We recognise that many of our pupils are on these apps regardless of age limits, which are often misunderstood or ignored. We therefore remind about best practice while remembering the reality for most of our pupils is quite different.
The Ofcom 'Children and parents: media use and attitudes report 2023' has also shown that YouTube remains the most used site or app among all under 18s and the reach of WhatsApp, TikTok and Snapchat increased yet further.
The report highlights that 20% of 3-4 year olds have access to their OWN mobile phone (let alone shared devices), rising to over 90 percent by the end of Primary Academy, and the vast majority have no safety controls or limitations to prevent harm or access to inappropriate material. At the same time, even 3 to 6 year olds are being tricked into 'selfgenerated' sexual content (Internet Watch Foundation Annual Report) while considered to be safely using devices in the home and the 7-10 year old age group is the fastest growing for this form of child sexual abuse material, up 60 percent within 12 months to represent over 60,000 cases found (of this same kind where the abuser is not present).

Main online safety trends to look out for in 2023/2024

Self-generative artificial intelligence has been a significant change, with children now having often unfettered access to tools that generate text and images at home or in academy. These tools not only represent a challenge in terms of accuracy when young people are genuinely looking for information, but also in terms of plagiarism for teachers and above all safety
In the past year, more and more children and young people used apps such as snapchat as their source of news and information, with little attention paid to the veracity of influencers sharing news. The 2023 Revealing-Reality: Antisocial-Media Report highlights that this content is interspersed with highly regular exposure to disturbing, graphic and illegal content such as fights, attacks, sexual acts and weapons. At the same time, the Children's Commissioner revealed the ever younger children are regularly consuming pornography and living out inappropriate behaviour and relationships due to 'learning from' pornography. This has coincided with the rise of misogynistic influencers such as Andrew Tate, which had a significant influence on many young boys over the past year.
Nationally there has been a significant increase in the number of fake profiles causing issues in schools, both for schools – where the school logo and/or name have been used to share inappropriate content about children and also spread defamatory allegations about staff.

Introduction and Overview

New technologies have become integral to the lives of children in today's society, both within the academy and in their lives outside the academy. Today's pupils are growing up in an increasingly complex world, living their lives seamlessly on and offline. The internet and other digital information technologies are powerful tools, which open up new opportunities for everyone. These technologies can create discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for all to be more creative and productive in their work. Such technologies do present challenges and risks. We want to equip our pupils with the knowledge needed to make the best use of the internet and technology in a safe, considered and respectful way so they can reap the benefits of the online world. This policy will underpin knowledge and behaviour in an age appropriate way to help pupils navigate the online world safely and confidently regardless of their device, platform or app. The academy makes it clear to pupils that even though the online space differs in many ways, the same standards of behaviour are expected online as apply offline, and that everyone should be treated with kindness, respect and dignity.

Online safety is an integral part of safeguarding and requires a whole academy, cross-curricular approach and collaboration between key academy leads. Accordingly, this policy is written in line with 'Keeping Children Safe in Education' 2023 (KCSIE), 'Teaching Online Safety in Academies', statutory RSHE guidance and other statutory documents. It is cross-curricular (with relevance beyond Relationships, Health and Sex Education, Citizenship and Computing) and designed to sit alongside or be integrated into your academy's statutory Child Protection & Safeguarding Policy. Any issues and concerns with online safety must always follow the academy's safeguarding and child protection procedures.

The continued cost-of-living crisis has meant that children have spent more time online and therefore exposed to all manner of online harms as families have had to cut back on leisure activities and the public provision of free activities for young people has reduced further. Therefore the wide scale use of technology as a tool for learning, socialising and play the role of online safety at our academy continues to evolve and increase. We recognise that online safety is part of our statutory safeguarding responsibilities and we implement approaches which will safeguard our community online.

Aims

This policy aims to promote a whole academy approach to online safety by:

- Setting out expectations for all The Carlton Infant Academy community members' online behaviour, attitudes and activities and use of digital technology (including when devices are offline)
- Helping the safeguarding and senior leadership team to have a better understanding and awareness of all elements of online safeguarding through effective collaboration and communication with technical colleagues (e.g. for filtering and monitoring), curriculum leads (e.g. RSHE) and beyond.
- Helping all stakeholders to recognise that online/digital behaviour standards (including social media activity) must be upheld beyond the confines of the academy gates and academy day, regardless of device or platform, and that the same standards of behaviour apply online and offline.
- Facilitating the safe, responsible, respectful and positive use of technology to support teaching & learning, increase attainment and prepare children and young people for the risks and opportunities of today's and tomorrow's digital world, to survive and thrive online
- Helping academy staff working with children to understand their roles and responsibilities to work safely and responsibly with technology and the online world:
    - for the protection and benefit of the children and young people in their care, and
    - for their own protection, minimising misplaced or malicious allegations and to better understand their own standards and practice
    - for the benefit of the academy, supporting the academy ethos, aims and objectives, and protecting the reputation of the academy and profession
- Establishing clear structures by which online misdemeanours will be treated, and procedures to follow where there are doubts or concerns (with reference to other academy policies such as Behaviour Policy or Anti-Bullying Policy)

<u>The main areas of risk for our academy community can be categorised into four areas of risk</u>:

Content

Being exposed to illegal, inappropriate or harmful content, for example:

- Online pornography, fake news, racism, misogyny, anti-Semitism, radicalisation and extremism.
- Ignoring age ratings in games (exposure to violence associated with often racist language) and substance abuse.
- Lifestyle websites, for example pro-anorexia/self-harm/suicide sites.
- Hate sites.
- Content validation: How to check authenticity and accuracy of online content.

Contact

Being subjected to harmful online interaction with other users; for example:

- Adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.
- Child-on-Child abuse.
- Online-bullying in all forms.
- Identity theft (including Facebook hijacking) and sharing passwords.

Conduct

Personal online behaviour that increases the likelihood of, or causes, harm; for example:

- Privacy issues, including disclosure of personal information.
- Digital footprint and online reputation.
- Health and well-being (amount of time spent online or gaming).
- Making, sending and receiving explicit images. e.g consensual and non-consensual sharing of nudes and seminudes and/or pornography.
- Sexual harassment.
- Sharing other explicit images.
- Online bullying.
- Extremism/radicalisation.
- Copyright (little care or consideration for intellectual property and ownership – such as digital images and video, music and film).

Commerce

Being exposed to financial risks such as:

- Online gambling.
- Inappropriate advertising.
- Commercial advertising.
- Phishing.
- Financial scams.

Scope of the policy

This policy applies to all members of The Carlton Infant Academy community (including teaching, supply and support staff, governors, volunteers, contractors, trainees, pupils, parents/carers, visitors and community users) who have access to our digital technology, networks and systems, whether on-site or remotely, and at any time, or who use technology in their academy role.

Roles and responsibilities

All stakeholders have a duty to behave respectfully online and offline, to use technology for teaching and learning and to prepare pupils for life after academy, and to immediately report any concerns or inappropriate behaviour, to protect staff, pupils, families and the reputation of the academy. We learn together, make honest mistakes together and support each other in a world that is online and offline at the same time. Depending on their role, all members of the academy community have individual roles and responsibilities, including in filtering and monitoring. All staff have a key role to play in feeding back on potential issues.

All staff

All staff sign and follow the staff Acceptable Use Policy in conjunction with this policy, the safeguarding policy, the code conduct/handbook and relevant parts of Keeping Children Safe in Education to support a whole-academy safeguarding approach. This includes reporting any concerns, no matter how small, to the Safeguarding Team, maintaining an awareness of current online safety issues, guidance (such as KCSIE), attending online safety training and reading email updates, modelling safe, responsible and professional behaviours in their own use of technology, avoiding scaring, victim-blaming language. They should take into account local context and any specific vulnerabilities for learners e.g. children with SEND or mental health needs, children in care or children who have experienced abuse.

In line with the DfE standards and the relevant changes to filtering and monitoring, staff will play their part in feeding back about over-blocking, gaps in provision or pupils bypassing protections. From time-to-time, for good educational reasons, pupils may need to research topics (eg racism, drugs and discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Computing Leader arranges for the temporarily removal of sites from the filtered list for the period of study, and with permission from the Headteacher. Any request to do so, should be auditable, with clear reasons for the need. When pupils are allowed to search the internet, staff should be vigilant in monitoring the content of the websites seen. Pupils should have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations. They should also recap the online safety rules so that any content that bypasses a filter can be dealt with quickly and effectively. Staff need to help children understand and follow the Online Safety Policy and Acceptable Use Policies. If remote learning is being undertaken or devices are being used at home, it should be done so safely and in line with policy.

Governors

Governors are responsible for approving and reviewing the Online Safety Policy. Governors receive regular information about online safety incidents and reports at LAB meetings. Claire Whiteside is the Online Safety Governor with responsibility for over-seeing filtering and monitoring.

Key responsibilities of the Online Safety Governor and Safeguarding Link Governor.

- Approve this policy and strategy and subsequently review its effectiveness, e.g. by asking the questions in the helpful document from the UK Council for Child Internet Safety (UKCIS) Online safety in academies and colleges: Questions from the Governing Board

- Undergo (and signpost all other governors and to attend) safeguarding and child protection training (including online safety) at induction to provide strategic challenge and into policy and practice, ensuring this is regularly updated.
- Ensure that all staff also receive appropriate safeguarding and child protection (including online) training at induction and that this is updated.
- Support the academy in encouraging parents and the wider community to become engaged in online safety activities.
- Have regular strategic reviews with the online-safety coordinator/DSL and incorporate online safety into standing discussions of safeguarding at governor meetings.
- Work with the Data Protection Officer, DSL(HT) to ensure a compliant framework for storing data, but helping to ensure that child protection is always put first and data-protection processes support careful and legal sharing of information.
- Check all staff have read Part 1 of KCSIE; SLT and all working directly with children have read Annex B.
- Ensure that all staff undergo safeguarding and child protection training, including online safety and now also reminders about filtering and monitoring.
- Ensure that children are taught about safeguarding, including online safety as part of providing a broad and balanced curriculum which demonstrates a whole academy approach to online safety and use of mobile technology.

Head teacher

As all staff, plus:

- Foster a culture of safeguarding where online-safety is fully integrated into whole-academy safeguarding.
- Oversee and support the activities of the safeguarding team and ensure they work with technical colleagues to complete an online safety audit in line with KCSIE.
- Undertake training in offline and online safeguarding, in accordance with statutory guidance and Local Safeguarding Children Partnership support and guidance.
- Ensure ALL staff undergo safeguarding training (including online-safety) at induction and with regular updates and that they agree and adhere to policies and procedures.
- Ensure ALL governors undergo safeguarding and child protection training and updates (including online-safety) to provide strategic challenge and oversight into policy and practice and that governors are regularly updated on the nature and effectiveness of the academy's arrangements.
- Ensure the academy implements and makes effective use of appropriate ICT systems and services including academy-safe filtering and monitoring, protected email systems and that all technology including remote systems are implemented according to child-safety first principles.
- Better understand, review and drive the rationale behind decisions in filtering and monitoring as per DfE standards —through regular liaison with technical colleagues and the DSL– in particular understand what is blocked or allowed for whom, when, and how as per KCSIE. This now involves starting regular checks and annual reviews, upskilling the DSL and appointing a filtering and monitoring governor.
- Liaise with colleagues on all online-safety issues which might arise and receive regular updates on academy issues and broader policy and practice information.
- Support the safeguarding team and technical staff as they review protections for pupils in the home and remote learning procedures, rules and safeguards.

- Take overall responsibility for data management and information security ensuring provision follows best practice in information handling; work with the DPO and governors to ensure a compliant framework for storing data, but helping to ensure that child protection is always put first and data-protection processes support careful and legal sharing of information.
- Understand and make all staff aware of procedures to be followed in the event of a serious online safeguarding incident.
- Ensure suitable risk assessments are undertaken so the curriculum meets pupil needs, including risk of children being radicalised.
- Monitor the use of technology, online platforms and social media presence and that any misuse/attempted misuse is identified and reported in line with policy.
- Ensure the academy website meets statutory requirements.

Safeguarding Team / Online Safety Lead

- Support and assist the DSL/HT to secure an effective whole academy approach to online safety as per KCSIE including the requirements for filtering and monitoring.
- Work to take up the new responsibility for filtering and monitoring by working closely with technical colleagues, SLT and the new filtering governor to learn more about this area, better understand, review and drive the rationale behind systems in place and initiate regular checks and annual reviews, including support for devices in the home.
- Where online-safety duties are delegated and in areas of the curriculum where the DSL is not directly responsible but which cover areas of online safety (e.g. PSHRE), ensure there is regular review and open communication and that the DSL's clear overarching responsibility for online safety is not compromised or messaging to pupils confused
- Ensure ALL staff and supply staff undergo safeguarding and child protection training (including online-safety) at induction and that this is regularly updated. ○ This must include filtering and monitoring and help them to understand their roles ○ All staff must read KCSIE Part 1 and Annex B ○ Cascade knowledge of risks and opportunities throughout the organisation
- Ensure that ALL governors and undergo safeguarding and child protection training (including online-safety) at induction to enable them to provide strategic challenge and oversight into policy and practice and that this is regularly updated.
- Take day-to-day responsibility for safeguarding issues and be aware of the potential for serious child protection concerns.
- Be mindful of using appropriate language and terminology around children when managing concerns, including avoiding victim-blaming language.
- Remind staff of safeguarding considerations as part of a review of remote learning procedures and technology, including that the same principles of online-safety and behaviour apply.
- Work closely with SLT, staff and technical colleagues to complete an online safety audit (including technology in use in the academy).
- Work with the Headteacher, DPO and governors to ensure a compliant framework for storing data, but helping to ensure that child protection is always put first and data-protection processes support careful and legal sharing of information.
- Stay up to date with the latest trends in online safeguarding and "undertake Prevent awareness training."
- Review and update this policy, other online safety documents (e.g. Acceptable Use Policies) and the strategy on which they are based (in harmony with policies for behaviour, safeguarding, Prevent and others) and submit for review to the governors.

- Receive regular updates in online-safety issues and legislation, be aware of local and academy trends.
- Ensure that online-safety education is embedded across the curriculum in line with the statutory RSHE guidance
- Promote an awareness of and commitment to online-safety throughout the academy community, with a strong focus on parents, including hard-to-reach parents.
- Communicate regularly with SLT and the safeguarding governor/committee to discuss current issues (anonymised), review incident logs and filtering/change control logs and discuss how filtering and monitoring work and have been functioning/helping.
- Ensure all staff are aware of the procedures that need to be followed in the event of an online safety incident, and that these are logged in the same way as any other safeguarding incident.
- Ensure staff adopt a zero-tolerance, whole academy approach to all forms of child-on-child abuse, and don't dismiss it as banter (including bullying).
- Take into account local content and any specific vulnerabilities for learners e.g. children with SEND or mental health needs, children in care or children who have experienced abuse.
- Receive reports of online safety incidents and creates a log of incidents to inform future online safety developments.
- Consult with stakeholders, including parents/carers and pupils about online safety provision so that the academy can capture information about experiences of emerging issues.

PSHRE Lead:

- Embed consent, mental wellbeing, healthy relationships and staying safe online as well as raising awareness of the risks/challenges from recent trends in self-generative artificial intelligence, financial extortion and sharing intimate pictures online into the PSHRE curriculum. This will include being taught what positive, healthy and respectful online relationships look like, the effects of their online actions on others and knowing how to recognise and display respectful behaviour online. Throughout PSHRE, teachers will address online safety and appropriate behaviour in an age appropriate way that is relevant to their pupils' lives.
- Focus on the underpinning knowledge and behaviours outlined in Teaching Online Safety in Schools in an age appropriate way to help pupils to navigate the online world safely and confidently regardless of their device, platform or app.
- Assess teaching to identify where pupils need extra support/intervention to complement the computing curriculum.
- Work closely with DSL and all other staff to ensure an understanding of the issues, approaches and messaging within PSHRE.
- Ensure that the PSHRE policy and outline of the curriculum is included on the academy website.
- Work closely with the Computing Lead to avoid overlap but ensure a complementary whole-academy approach, and with all other lead staff to embed the same whole-academy approach.

Computing Lead:

- Look for opportunities to embed online safety in the subject, especially as part of the PSHRE curriculum, and model positive attitudes and approaches to staff and pupils alike.

- Consider how the UKCIS framework Education for a Connected World and Teaching Online Safety in Schools can be applied in your subject.
- Work closely with the DSL/Computing lead to ensure an understanding of the issues, approaches and messaging within Computing.
- Ensure subject specific action plans also have an online-safety element.

Network Manager/Technical

- Collaborate regularly with DSL, Computing lead and SLT to support key strategic decisions around the safeguarding elements of technology.
  In regard to filtering and monitoring, the DSL and safeguarding team, to understand and manage School Broadband and SENSO Alerting Software and carry out regular reviews and annual checks.
- Support DSL/Computing lead to carry out an annual online safety audit. This should also include a review of technology, including filtering and monitoring systems including protecting pupils using school technology at home.
- Keep up to date with the academy Online Safety Policy and technical information in order to effectively carry out your online safety role and to inform and update others as relevant.
- Work closely with the DSL/online safety lead/data protection officer/PSHRE lead to ensure that systems and networks reflect policy and there are no conflicts between educational messages and practice.
- Ensure the above stakeholders understand the consequences of existing services and of any changes to these systems (especially in terms of access to personal and sensitive records/data and to systems such as YouTube mode, web filtering settings, sharing permissions for files on cloud platforms etc.
- Maintain up-to-date documentation of the academy online security and technical procedures.
- Report online-safety related issues that come to your attention in line with academy policy to the Headteacher/safeguarding team.
- Manage the academy systems, networks and devices, according to a strict password section of this policy, with systems in place for detection of misuse and malicious attack, with adequate protection, encryption and backup for data, including disaster recovery plans, and auditable access controls.
- Ensure the Cybersecurity Policy is up to date, easy to follow and practicable

Data protection officer

- Provide data protection expertise, training and support for implementing the Data Protection and Cyber Security Policy and ensure that the policies conform with each other and with this policy.
- Not prevent, or limit, the sharing of information for the purposes of keeping children safe. As outlined in Data protection in schools, 2023, “It’s not usually necessary to ask for consent to share personal information for the purposes of safeguarding a child.” And in KCSIE 2023, “The Data Protection Act 2018 and UK GDPR do not prevent the sharing of information for the purposes of keeping children safe. Fears about sharing information must not be allowed to stand in the way of the need to safeguard and promote the welfare and protect the safety of children.”
- Note that retention schedules for safeguarding records may be required to be set as ‘Very long term need (until pupil is aged 25 or older)’.

- Ensure that all access to safeguarding data is limited as appropriate, and also monitored and audited.

Visitors and contractors:

- Read, understand, sign and adhere to an Acceptable Use Policy (AUP).
- Report any concerns, no matter how small, to the DSL.
- Maintain an awareness of current online safety issues and guidance.
- Model safe, responsible and professional behaviours in their own use of technology at the academy and as part of remote teaching or any online communications.
- Note that as per AUP agreement a contractor will never attempt to arrange any meeting, **including tutoring session,** without the full prior knowledge and approval of the academy, and will never do so directly with a pupil. The same applies to any private/direct communication with a pupil.

Pupils:

- Read, understand and adhere to the student/pupil Acceptable Use Policy.
- Understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- Know and understand policies on the use of mobile devices. They should also know and understand policies on the taking/use of images and on online-bullying.
- Understand the importance of adopting good online safety practice when using digital technologies out of the academy and realising that the academy Online Safety Policy covers their actions out of the academy.

Parents/Carers

- Read, sign and adhere to the academy parental Acceptable Use Policy (AUP).
- Read the pupil AUP and encourage their children to follow.

Education and curriculum:

We have established a carefully considered and sequenced curriculum for online safety that builds on what pupils have already learned and identifies subject content that is appropriate for their stage of development. Our E-safety curriculum is embedded throughout our computing curriculum. The first 10-15 minutes of each lesson is dedication to whole class discussions surrounding the use of technology and E-Safety. The resources are tailored to the specific needs and risks of our pupils, including vulnerable pupils

As well as teaching the underpinning knowledge and behaviours that can help pupils navigate the online world safely and confidently regardless of the device, platform or app, we have embedded teaching about online safety and harms through a whole academy approach.

The following subjects have the clearest online safety links (see the relevant role descriptors above for more information):

- Personal, Social, Health and Relationships Education
- Computing

However, as stated in the role descriptors above, it is the role of all staff to identify opportunities to thread online safety through all learning and making the most of unexpected learning opportunities as they arise (which have a unique value for our pupils). We recognise that online safety and broader digital resilience must be thread throughout the curriculum and that is why we have a cross-curricular approach. There are annual reviews of curriculum plans and schemes of work to ensure we keep up to date with current online safety issues.

Whenever overseeing the use of technology (devices, the internet, new technology such as augmented reality, etc) in the academy or as homework tasks, all staff should encourage sensible use, monitor what pupils are doing and consider potential dangers and the age appropriateness of websites. Parents and carers are informed what systems we use to filter and monitor online use. They know what their child is being asked to do online, including the sites they access which are being filtered and monitored in line with KCSIE 2023

Equally, all staff carefully supervise and guide pupils when engaged in learning activities involving online technology (including, extra-curricular, extended academy activities if relevant and remote teaching), supporting them with search skills, critical thinking (e.g. disinformation, misinformation and fake news), age appropriate materials and signposting, and legal issues such as copyright and data law.

Handling safeguarding concerns and incidents

The use of technology has become a significant component of many safeguarding issues. Child sexual exploitation; radicalisation; sexual predation: technology often provides the platform that facilitates harm. An effective approach to online safety empowers our academy to protect and educate the whole academy community in their use of technology and establishes mechanisms to identify, intervene in, and escalate any incident where appropriate.

Online Safety safeguarding issues are dealt with in line with the Keeping Children Safe in Education 2023 and the following policies:

- Safeguarding and Child Protection Policy which makes reference to sexual harassment/child-on-child abuse policy
- Anti-Bullying and Behaviour Policies
- Acceptable Use Policies
- Prevent Risk Assessment
- Data Protection Policy, agreements and other documentation (e.g. privacy statement and consent forms for data sharing, image use etc)
- Cyber Security Policy

This Academy commits to take all reasonable precautions to ensure safeguarding pupils online, but recognises that incidents will occur both inside/outside the academy (and that those from outside the academy will continue to impact pupils when they come into the academy or during extended periods away from the academy). General concerns must be handled in the same way as any other safeguarding concern. Any suspected online risk or infringement should be reported to the DSL/safeguarding team in a timely manner.

Any concern/allegation about staff misuse is always referred directly to the Headteacher, unless the concern is about the Headteacher in which case the complaint is referred to the Chair of Governors, who follows policy. Staff may also use the NSPCC Whistleblowing Helpline.
We will inform parents/carers of online-safety incidents involving their children, and the Police where staff or pupils engage in or are subject to behaviour which we consider is particularly concerning or breaks the law (particular procedures are in place for sexting and upskirting; see section below).

The Academy will actively seek support from other agencies as needed (i.e. The Redhill Academy Trust, UK Safer
Internet Centre's Professionals' Online Safety Helpline (POSH), NCA CEOP, Prevent Officer, Police, IWF and Harmful
Sexual Behaviour Support Service). The DfE guidance Behaviour in Schools, advice for Headteachers and school staff September 2022 provides advice and related legal duties including support for pupils and powers of staff when responding to incidents.

Sharing Nudes and Semi-Nudes (Sexting)

In the latest advice(UKCIS, 2020), this is defined as the sending or posting of nude or semi-nude images, videos or live streams online by young people under the age of 18. NB - where one of the parties is over 18, this is no longer sexting but child sexual abuse.

This could be via social media, gaming platforms, chat apps or forums. It could also involve sharing between devices via services like Apple's AirDrop which works offline. Alternative terms used by children and young people may include 'dick pics' or 'pics'. The motivations for taking and sharing nude and semi-nude images, videos and live streams are not always sexually or criminally motivated.
This advice does not apply to adults sharing nudes or semi-nudes of under 18-year olds. This is a form of child sexual abuse and must be referred to the police as a matter of urgency.

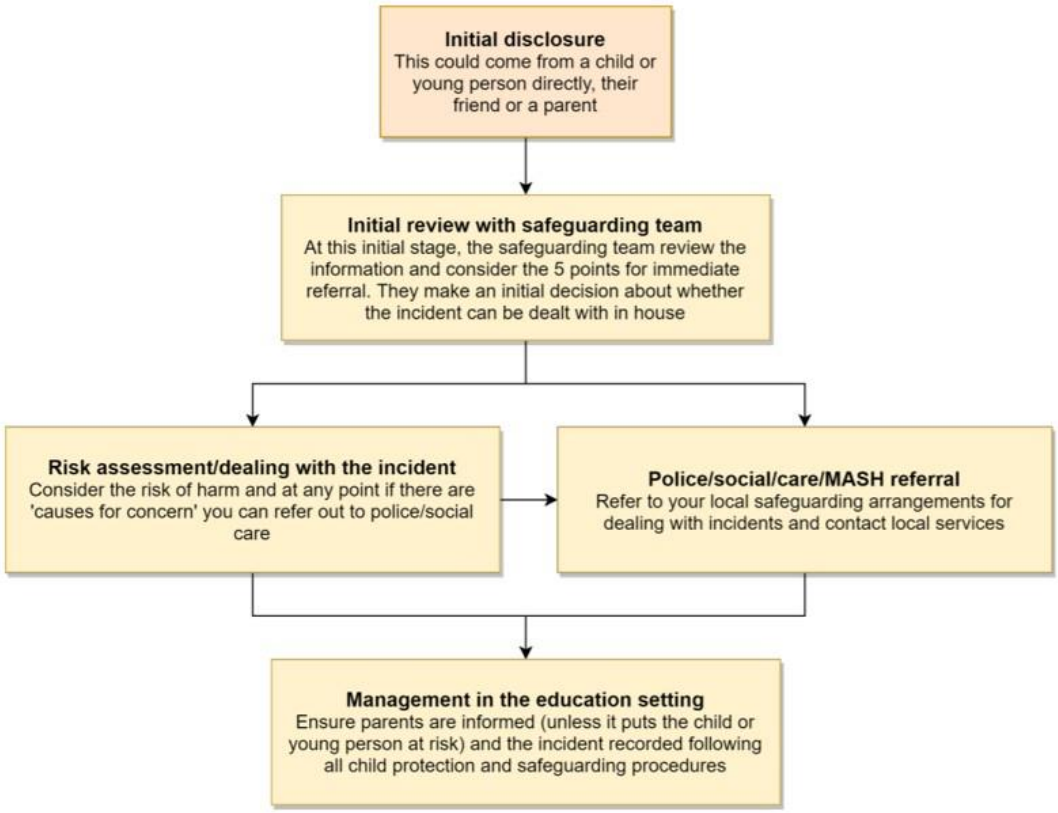
Guidance about dealing with self-generated images/sexting can be found at – UKSIC Responding to and managing sexting incidents and UKCIS – Sexting in schools and colleges

What to do if an incident involving 'sharing nudes or semi-nudes' comes to your attention:

- Report it to your Designated Safeguarding Lead (DSL) immediately.
- **Never** view, copy, print, share, store or save the imagery yourself**,** or ask a child to share or download – **this is illegal**.
- If you have already viewed the imagery by accident (e.g. if a young person has showed it to you before you could ask them not to), report this to the DSL (or equivalent) and seek support.
- **Do not** delete the imagery or ask the young person to delete it.
- **Do not** ask the child/children or young person(s) who are involved in the incident to disclose information regarding the imagery. This is the responsibility of the DSL (or equivalent).
- **Do not** share information about the incident with other members of staff, the young person(s) it involves or their, or other, parents and/or carers.
- **Do not** say or do anything to blame or shame any young people involved.
- **Do** explain to them that you need to report it and reassure them that they will receive support and help from the DSL (or equivalent). Our academy's safeguarding policies outline codes of practice to be followed.

The full guidance, Sharing nudes and semi-nudes: advice for education settings(UKCIS, 2020) can be found at www.gov.uk/government/publications/sharing-nudes-and-semi-nudes-advice-for-education-settings-working-withchildren-and-young-people.

The DSL will in turn use the full guidance document, Sharing nudes and semi-nudes – advice for educational settings to decide next steps and whether other agencies need to be involved.



Consider the 5 points for immediate referral at initial review:

1. The incident involves an adult
2. There is reason to believe that a child or young person has been coerced, blackmailed or groomed, or there are concerns about their capacity to consent (for example, owing to special educational needs)
3. What you know about the images or videos suggests the content depicts sexual acts which are unusual for the young person's developmental stage, or are violent
4. The images involves sexual acts and any pupil in the images or videos is under 13
5. You have reason to believe a child or young person is at immediate risk of harm owing to the sharing of nudes and semi-nudes, for example, they are presenting as suicidal or self-harming

It is important that everyone understands that whilst sexting is illegal, pupils can come and talk to members of staff if they have made a mistake or had a problem in this area.

Upskirting

Upskirting (taking a photo of someone under their clothing, not necessarily a skirt) is a criminal offence and constitutes a form of sexual harassment as highlighted in Keeping Children Safe in Education. As with other forms of child on child abuse pupils can come and talk to members of staff if they have made a mistake or had a problem in this area.

Bullying

Online bullying, including incidents that take place outside the academy or from home should be treated like any other form of bullying and the bullying policy should be followed.
It is important to be aware that in the past 12 months there has been an increase in anecdotal reports of fights being filmed and fake profiles being used to bully children in the name of others. When considering bullying, staff will be reminded of these issues, cyber bullying and not accepting banter.

Abuse and Neglect

All staff should be aware that technology is a significant component in many safeguarding and wellbeing issues. Children are at risk of abuse online as well as face-to-face. Abuse can take place wholly online, or technology may be used to facilitate offline abuse. In many cases abuse will take place concurrently via online channels and in daily life. Children can also abuse their peers online, this can take the form of abusive, harassing, and misogynistic messages, the nonconsensual sharing of indecent images, especially around chat groups, and the sharing of abusive images and pornography, to those who do not want to receive such content.

In all cases, if staff are unsure, they should always speak to the DSL (or deputy). Staff receive information and training which addresses online safety at induction, and as part of accessing regularly updated safeguarding and child protection training and information.

Indicators of Abuse and Neglect

Emotional abuse: the persistent emotional maltreatment of a child such as to cause severe and adverse effects on the child's emotional development. It may involve serious bullying, including cyberbullying.

Sexual abuse: involves forcing or enticing a child or young person to take part in sexual activities, not necessarily involving violence, whether or not the child is aware of what is happening. The activities may involve … non-contact activities, such as involving children in looking at, or in the production of, sexual images, watching sexual activities, encouraging children to behave in sexually inappropriate ways, or grooming a child in preparation for abuse. Sexual abuse can take place online, and technology can be used to facilitate offline abuse.

Child Sexual Exploitation (CSE)

CSE is a form of child sexual abuse. Sexual abuse may involve physical contact, including assault by penetration (for example, rape or oral sex) or non-penetrative acts such as masturbation, kissing, rubbing, and touching outside clothing. It may include noncontact activities, such as involving children in the production of sexual images, forcing children to look at sexual images or watch sexual activities, encouraging children to behave in sexually inappropriate ways or grooming a child in preparation for abuse including via the internet. CSE can occur over time or be a one-off occurrence and may happen without the child's immediate knowledge e.g. through others sharing videos or images of them on social media.

Child-on-Child Abuse

All staff are aware that children can abuse other children and that it can happen both inside/outside of the academy and online. All staff recognise the indicators and signs of peer on peer abuse and know how to identify it and respond to reports. All staff understand, that even if there are no reports in the academy it does not mean it is not happening, it may be the case that it is just not being reported. As such it is important if staff have any concerns regarding child-onchild abuse, they should speak to the DSL or safeguarding team. This is especially likely to be the case where there is online abuse concerns. For example learners frequently report they are unlikely to report concerning online behaviours if they are using what adults consider to be 'inappropriate' social media platforms or gaming sites. Staff understand the importance of challenging inappropriate behaviours which take place online.

Child-on-child online abuse is most likely to include, but may not be limited to:

- Bullying (including cyberbullying, prejudice-based and discriminatory bullying).
- Physical abuse such as hitting, kicking, shaking, biting, hair pulling, or otherwise causing physical harm (this may include an online element which facilitates, threatens and/or encourages physical abuse).
- Sexual violence, such as rape, assault by penetration and sexual assault; (this may include an online element which facilitates, threatens and/or encourages sexual violence).
- Sexual harassment, such as sexual comments, remarks, jokes and online sexual harassment, which may be standalone or part of a broader pattern of abuse.
- Causing someone to engage in online sexual activity without consent, such as forcing someone to strip, touch themselves sexually, or to engage in sexual activity with a third party.
- Consensual and non-consensual sharing of nudes and semi-nude images and or videos (also known as sexting or youth produced sexual imagery).
- Upskirting, which typically involves taking a picture under a person's clothing without their permission, with the intention of viewing their genitals or buttocks to obtain sexual gratification, or cause the victim humiliation, distress or alarm. This can then be shared online.
- Initiation/hazing type violence and rituals (this could include activities involving harassment, abuse or humiliation used as a way of initiating a person into a group and may also include an online element).

Child-on-child sexual violence and sexual harassment

Any incident of sexual harassment or violence (online/offline) should be reported to the DSL who will follow the full guidance. Staff should work to foster a zero-tolerance culture, where sexual violence and sexual harassment are never acceptable, will not be tolerated and will maintain an attitude of 'it could happen here'. The academy takes all forms of sexual violence and harassment seriously and behaviours incorrectly viewed as 'low level' are treated seriously and not allowed to perpetuate. Part 5 of Keeping Children Safe in Education covers 'Child-on-child sexual violence and sexual harassment'.

In the online environment, the recent proliferation of misogynistic content is particularly relevant when it comes to considering reasons for and how to combat this kind of behaviour. The Academy

undertakes Pupil Voice Surveys and listens carefully for careless use of language to see if children are being influenced for example by online influencers and people like Andrew Tate. Staff challenge the inappropriate language and behaviour between pupils.

County Lines

County lines is a term used to describe gangs and organised criminal networks involved in exporting illegal drugs using dedicated mobile phone lines or other form of "deal line". This activity can happen locally as well as across the UK - no specified distance of travel is required. Children and vulnerable adults are exploited to move, store and sell drugs and money. Offenders will often use coercion, intimidation, violence (including sexual violence) and weapons to ensure compliance of victims. Children are also increasingly being targeted and recruited online using social media.

Preventing Radicalisation

Children are vulnerable to extremist ideology and radicalisation online. The internet can be used as a tool for radicalisation and in the potential accidental and deliberate exposure to extremist views and content online. Similar to protecting children from other forms of harms and abuse, protecting children from this risk is part of the safeguarding and online safety approach. There is no single way of identifying whether a child is likely to be susceptible to an extremist ideology. Background factors combined with specific influences such as family and friends may contribute to a child's vulnerability. Similarly, radicalisation can occur through many different methods (such as social media or the internet) and settings (such as within the home). However, it is possible to protect vulnerable people from extremist ideology and intervene to prevent those at risk of radicalisation being radicalised.

Cybercrime

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

- Unauthorised access to computers (illegal 'hacking'), for example accessing an academy's computer network to look for test paper answers or change grades awarded.

- Denial of service attacks (A denial-of-service (DoS) attack floods a server with traffic, making a website or resource unavailable.
A distributed denial-of-service (DDoS) attack is a DoS attack that uses multiple computers or machines to flood a targeted resource) or 'booting'. These are attempts to make a computer, network or website unavailable by overwhelming it with internet traffic from multiple sources.

- Making, supplying or obtaining malware (malicious software) such as viruses, spyware, ransomware, botnets and Remote Access Trojans with the intent to commit further offence, including those above.

Children with particular skill and interest in computing and technology may inadvertently or deliberately stray into cyber-dependent crime. If there are concerns about a child in this area, the DSL (or a deputy), should consider referring into the Cyber Choices Programme. This is a nationwide police programme supported by the Home Office and led by the National Crime Agency, working with regional and local policing. It aims to intervene where young people are at risk of committing, or being drawn into, low level cyber-dependent offences and divert them to a more positive use of their skills and interests.

Data Protection

All pupils, staff, governors, volunteers, contractors and parents are bound by the academy data protection and cybersecurity Policy. It is important to remember that there is a close relationship between both data protection and cybersecurity and the ability to effectively safeguard children. Data protection does not prevent, or limit, the sharing of information for the purposes of keeping children safe. As outlined in Data protection in schools 2023, "It's not usually necessary to ask for consent to share personal information for the purposes of safeguarding a child." And in KCSIE 2023, "The Data Protection Act 2018 and UK GDPR do not prevent the sharing of information for the purposes of keeping children safe. Fears about sharing information must not be allowed to stand in the way of the need to safeguard and promote the welfare and protect the safety of children."

Passwords:

The Carlton Infant Academy:

- Ensures all staff have their own unique username and private passwords to access academy systems which are changed on a regular basis.
- All staff use passwords that are three random words and over 12 characters in length.
- Ensures all staff passwords do not include names or any other personal information about the user that might be known by others.
- Allows staff to change their password on first login to the system.
- Makes it clear that staff and pupils must always keep their password private, must not share it with others and must not leave it where others can find it.
- Ensures that pupils have their own unique username to access their work area on the server.
- Ensures that pupils have their own unique password and username for online teaching platforms

Technical support:

The academy works with GBMicros who ensure that the academy is as secure as possible with the current systems that are in place. In regards to the anti-virus the academy uses ESET. This will ensure that the anti-virus is then fully maintained and monitored.

The current systems ensure that:

- Users can only access data to which they have right of access.
- No user can access another's files in their home area.
- Access to personal data is securely controlled in line with the academy's personal data policy.
- There is effective guidance and training for users.
- There is monitoring from senior leaders and these have impact on policy and practice.
- Academy technical systems are managed in ways that ensure the academy meets recommended technical requirements.
- There will be regular reviews and audits of the safety and security of the academy's technical systems.
- Servers, wireless systems and cabling are securely located and physical access restricted.
- Appropriate security measures are in place to protect the servers, firewalls, switches, routers, wireless systems, work stations, mobile devices etc. From accidental or malicious attempts which might threaten the security of the academy systems and data.

- Responsibilities for the management of technical security are clearly assigned to GBMicros.
- All users will have clearly defined access rights to academy technical systems.
- Users will be made responsible for the security of their username and password and must not allow other users to access the systems using their log-in details and must immediately report any suspicion or evidence that there has been a breach of security.
- The domain/administrator passwords for the ICT systems, used by the network manager will be handed over by GBMicros when GBMicros no longer supports the system. This is to keep access of key areas to an absolute minimum.
- GBMicros are responsible for ensuring that software licence logs are accurate, up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations.
- Technical staff regularly monitor and record the activity of users on the technical systems and users are made aware of this in the Acceptable Use Agreement.
- Remote management tools are used by staff to control workstations and view user's activity.
- An appropriate system is in place for users to report any actual/potential technical incident to the Computing lead or technician.
- The academy has regular maintenance evenings where workstations are protected by up-to-date software to protect against malicious threats from viruses.
- An agreed procedure is in place that forbids staff from downloading executable files and installing programmes on academy devices.
- An agreed procedure is in place regarding the use of removable media (e.g. memory sticks/CDs/DVDs) by users on academy devices.

Appropriate filtering and monitoring

The Academy follows the DfE filtering and monitoring standards, and we:

- Identify and assign roles and responsibilities to manage filtering and monitoring systems
- Review filtering and monitoring provision at least annually
- Block harmful and inappropriate content without unreasonably impacting teaching and learning
- Have effective monitoring strategies in place that meet their safeguarding needs

All staff are aware of the changes and renewed emphasis and play their part in feeding back about areas of concern, potential for pupils to bypass systems and any potential over blocking. They can submit concerns to the academy office and these are then passed on to GBMicros and the Headteacher so that the appropriate actions are taken. They are recorded and kept in the Online Safety Reporting Folder.

Staff will be reminded of the systems in place and their responsibilities at induction and start of year safeguarding as well as via AUPs and regular training reminders in the light of the annual review and regular checks that will be carried out.

At The Carlton Infant Academy:

- Web filtering is provided by Schools Broadband called Netsweeper on academy site and for academy devices used in the home
- Changes can be made by GBMicros
- Overall responsibility is held by the DSL

- Technical support and advice, setup and configuration are from Nicole Lang and GBMicros
- Regular checks are made half termly by Anna Scrivens, Nicole Lang and GBMicros to ensure filtering is still active and functioning everywhere.
- An annual review is carried out during our Cybersecurity review.

According to the DfE standards, "a variety of monitoring strategies may be required to minimise safeguarding risks on internet connected devices and may include:

- Physically monitoring by staff watching screens of users
- Live supervision by staff on a console with device management software
- Network monitoring using log files of internet traffic and web access

Individual device monitoring through the SENSO software or third-party services

At The Carlton Infant Academy, we use Netsweeper provided by school's broadband and SENSO software.

- Internet access is filtered for all users. Illegal content (child sexual abuse images) is currently filtered by School Broadband.
- SENSO Alerting Software is loaded on all Window devices which monitors all activity on devices and alerts Anna Scrivens, Amie Shaw and Nicole Lang.
- Internet filtering/monitoring should ensure that children are safe from terrorist and extremist material when accessing the internet.
- The academy has provided enhanced and differentiated user-level filtering. An agreed procedure is in place for the provision of temporary access of "guests" (e.g. trainee teachers, supply teachers, visitors) onto systems.
- To regularly review the effectiveness of the filtering and monitoring systems in place.

Electronic Devices – Searching Screening and Confiscation

In line with the DfE guidance 'Searching, screening and confiscation: advice for schools', the Headteacher and staff authorised by her, have a statutory power to search pupils/property on academy premises. This includes the content of mobile phones and other devices, for example as a result of a reasonable suspicion that a device contains illegal or undesirable material and material intended to cause harm, including but not exclusive to sexual images, pornography, violence or bullying.

As with all prohibited items, staff should first consider the appropriate safeguarding response if they find images, data or files on an electronic device that they reasonably suspect are likely to put a person at risk. Staff may examine any data or files on an electronic device they have confiscated as a result of a search if there is good reason to do so as defined in the guidance as: ○ poses a risk to staff or pupils;

○ is prohibited, or identified in the academy rules for which a search can be made or ○ is evidence in relation to an offence.

Searching with consent - Authorised staff may search with the learner's consent for any item
Searching without consent - Authorised staff may only search without the learner's consent for anything which is either 'prohibited' (as defined in Section 550AA of the Education Act 1996) or appears in the academy rules as an item which is banned.

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of pupils when they are off the academy 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 academy but is linked to membership of the academy. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. If the phone contains a pornographic image, Headteachers have a statutory power to search or seize a pupils' phone. The academy 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 the academy.

In carrying out the search:

- The authorised member of staff must have reasonable grounds for suspecting that a pupil is in possession of a mobile phone/personal electronic device.
- The authorised member of staff should take reasonable steps to check the ownership of the mobile phone/personal electronic device before carrying out a search.
- The authorised member of staff should go only as far as is reasonably necessary to establish the facts of the incident.
- The authorised member of staff should take care that, where possible, searches should not take place in public places e.g. an occupied classroom, which might be considered as exploiting the learner being searched.
- A pupil's mobile phone/personal electronic device can only be searched in the presence of the pupil and another member of staff, if at all possible, they too should be the same gender as the learner being searched.
- There is a limited exception to this rule: Authorised staff can carry out a search of a learner of the opposite gender including without a witness present, but only where you reasonably believe that there is a risk that serious harm will be caused to a person if you do not conduct the search immediately and where it is not reasonably practicable to summon another member of staff.

Extent of the search:

The person conducting the search may not require the learner to remove any clothing other than outer clothing, (outer clothing includes hats; shoes; boots; coat; blazer; jacket; gloves and scarves). The power to search without consent enables a personal search, involving removal of outer clothing and searching of pockets; but not an intimate search going further than that, which only a person with more extensive powers (e.g. a police officer) can do.
Use of Force – force cannot be used to search without consent for items banned under the academy rules regardless of whether the rules say an item can be searched for.

If the member of staff conducting the search suspects they may find an indecent image of a child (nude or semi-nude images), the member of staff should never intentionally view the image, and must never copy, print, share, store or save such images. When an incident might involve an indecent image of a child and/or video, the member of staff should confiscate the device, avoid looking at the device and refer the incident to the DSL(or deputy) as the most appropriate person to advise on the response. Handling such reports or concerns can be especially complicated and the Academy would follow the principles as set out in Keeping children safe in education.

If a member of staff finds any image, data or file that they suspect might constitute a specified offence, then they must be delivered to the police as soon as is reasonably practicable.

In exceptional circumstances the Headteacher may dispose of the image or data if there is a good reason to do so. In determining a 'good reason' to examine or erase the data or files, the Headteacher must have regard to the following guidance issued by the Secretary of State:

- In determining whether there is a 'good reason' to examine the data or files, the Headteacher should reasonably suspect that the data or file on the device has been, or could be used, to cause harm, undermine the safe environment of the academy and disrupt teaching, or be used to commit an offence.
- In determining whether there is a 'good reason' to erase any data or files from the device, the Headteacher should consider whether the material found may constitute evidence relating to a suspected offence. In those instances, the data or files should not be deleted, and the device must be handed to the police as soon as it is reasonably practicable. If the data or files are not suspected to be evidence in relation to an offence, a member of staff may delete the data or files if the continued existence of the data or file is likely to continue to cause harm to any person and the pupil and/or the parent refuses to delete the data or files themselves

The Academy also considers their duty of care responsibility in relation to those staff who may access disturbing images or other inappropriate material whilst undertaking a search. Seeing such material can be most upsetting. Advice would be sort on how best to support such staff.

A record should be kept of the reasons for the deletion of data/files. (a log sheet can be found in the appendices to the Online Safety Policy) This policy will be reviewed by the head teacher and governors annually and in response to changes in guidance and evidence gained from the records.

Care of confiscation devices:

In line with the behaviour policy, devices must not be brought in to the Academy. Therefore, the academy will request that parents/carers collect devices and will take no responsibility for the care/condition of confiscated items

Personal devices

Pupils are not allowed to bring mobile phones or other personal electronic devices, or use them in the academy. They must be left at the academy office on arrival and collected at the end of the academy day. If a pupil needs to contact parents/carers, they will be allowed to use an academy phone. Pupils should protect their phone numbers by only giving them to trusted friends and family members. Pupils will be instructed in safe and appropriate use of mobile phones and personally-owned devices and will be made aware of boundaries and consequences.

The sanctions for breaking these rules will be:

- The device will be removed from the children and taken to the academy office.
- Parents/Carers will be informed.
- **All staff** should leave their mobile phones/digital devices on silent and only use them in private staff areas during academy hours. Child/staff data should never be downloaded onto a private phone. If a staff member is expecting an important personal call when teaching or otherwise on duty, they may leave their phone with the academy office to answer on their behalf or ask the Headteacher for permission.

- The academy accepts no responsibility or liability in respect of lost, stolen or damaged devices while at the academy or on activities organised or undertaken by the academy.
- The academy reserves the right to search the content of any mobile phones and mobile devices on the premises where there is a reasonable suspicion that it may contain undesirable material, including those which promote pornography, violence or bullying.
- Bluetooth or similar functions of mobile phones and mobile devices should not be used to send digital/video images or files to other mobile phones.
- Staff should be mindful of the age limits for apps and software on their devices and should not use inappropriate age rated sites/apps in the academy.
- Where staff members are required to use a mobile phone for academy duties, for instance in case of emergency during off-site activities, or for contacting students or parents, then they should use their own device and hide (by inputting 141) their own mobile number to avoid a parent or student accessing a teacher's private phone number.
- If a member of staff breaches the academy AUP Policy, then disciplinary action may be taken.

Volunteers, contractors, governors should keep their phones out of sight and on silent. Under no circumstances should they be used in the presence of children or to take photographs or videos. If this is required (e.g. for contractors to take photos of equipment or buildings), permission of the Headteacher should be sought (the Headteacher may choose to delegate this) and this should be done in the presence of a member staff.

Parents are asked to leave their phones out of sight and turned on silent when they are in the academy building. They should ask permission before taking any digital images or videos, e.g. of displays in corridors or classrooms, and not capture other children. When at academy events, please refer to the Digital images and video section of this document on page. When parents are in the playground for drop-off/collection or on the academy grounds they should ask permission before taking any digital images or videos. Parents are advised, if they need to contact their child during the academy day, to contact the academy office.

Use of academy devices

Staff and pupils are expected to follow the terms of the academy policies for appropriate use and behaviour when on academy devices, whether on site or at home.

- Academy devices are not to be used in any way which contravenes AUPs, behaviour policy / staff code of conduct.
- Wifi is accessible for academy-related internet use / limited personal use. All such use is monitored.
- Academy devices for staff or students are restricted to the apps/software installed by the academy, whether for use at home or academy, and may be used for learning and reasonable as well as appropriate personal use.
- All and any usage of devices and/or systems and platforms may be tracked.

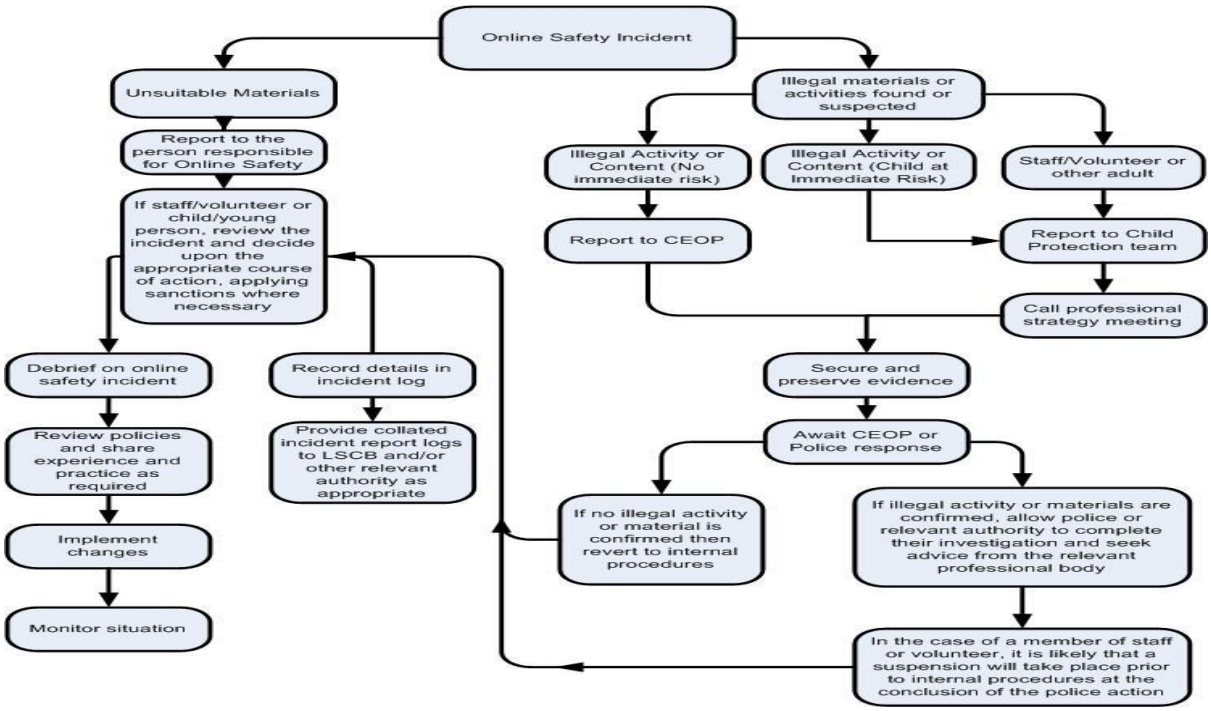
Misuse of academy technology

Clear and well communicated rules and procedures are essential to govern pupil and adult use of academy networks, connections, internet connectivity and devices, cloud platforms and social media (both when on site and outside of the academy).

These are defined in the relevant Acceptable Use Policy as well as in this document, for example in the sections relating to the professional and personal use of academy platforms/networks/clouds, devices and other technology, as well as to BYOD (bring your own device) policy. Where pupils contravene these rules, the behaviour policy will be applied; where staff contravene these rules, action will be taken as outlined in the staff code of conduct/handbook. It will be necessary to reinforce these as usual at the beginning of any academy year but also to remind pupils that the same applies for any home learning. Further to these steps, the academy reserves the right to withdraw – temporarily or permanently – any or all access to such technology, or the right to bring devices onto academy property.

Illegal incidents

If there is any suspicion that the website(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) for responding to online safety incidents and report immediately to the police.



Other Incidents

It is hoped that all members of the academy community will be responsible users of digital technologies, who understand and follow 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 form (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated the group 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 of Redhill Academy Trust 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.
- 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 academy 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.

Academy Actions & Sanctions

It is more likely that the academy 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 academy community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour/disciplinary procedures as follows:

Pupil Incidents	Refer to Headteacher/Online Safety Lead	Refer to Police	Refer to technical support staff for action re filtering/security etc.	Inform parents/carers	Removal of network/internet access rights	Further sanction eg detention/exclusion

Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable/inappropriate activities).	X	X	X	X	X	X
Unauthorised use of non-educational sites during lessons	X		X	X	X	X
Unauthorised/inappropriate use of mobile phone / digital camera/other mobile device	X		X	X	X	X
Unauthorised/inappropriate use of social media / messaging apps/personal email	X		X	X	X	X
Unauthorised downloading or uploading of files	X		X	X	X	X
Allowing others to access academy network by sharing username and passwords	X		X	X	X	X
Attempting to access or accessing the academy network, using another student's pupil's account	X		X	X	X	X
Attempting to access or accessing the academy network, using the account of a member of staff	X		X	X	X	X
Corrupting or destroying the data of other users	X		X	X	X	X
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	X	X	X	X	X	X
Actions which could bring the academy into disrepute or breach the integrity of the ethos of the academy	X	X	X	X	X	X
Using proxy sites or other means to subvert the academy's filtering system	X		X	X	X	X
Accidentally accessing offensive or pornographic material	X		X	X		
Deliberately accessing or trying to access offensive or pornographic material	X	X	X	X	X	X
Receipt or transmission of material that infringes the copyright of another person or infringes GDPR	X		X	X	X	X

Staff Incidents	Refer to Headteacher/Online Safety Lead	Refer to Local Authority	Refer to Police	Refer to Technical Support	Warning	Disciplinary Action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable/inappropriate activities)	X	X	X	X		X
Inappropriate personal use of the internet/social media/personal email	X	X	X	X	X	X
Unauthorised downloading or uploading of files	X			X	X	X
Allowing others to access academy network by sharing username and passwords or attempting to access or accessing the academy network, using another person's account	X			X	X	X
Careless use of personal data e.g. holding or transferring data in an insecure manner	X	X		X	X	X
Deliberate actions to breach data protection or network security rules	X			X	X	X
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	X		X	X	X	X
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	X	X	X	X	X	X
Using personal email/social networking/instant messaging/text messaging to carrying out digital communications with pupils	X	X	X	X	X	X
Actions which could compromise the staff member's professional standing	X	X	X	X	X	X
Actions which could bring the academy into disrepute or breach the integrity of the ethos of the academy	X	X	X	X	X	X

Using proxy sites or other means to subvert the academy's filtering system	X		X	X	X	X
Accidentally accessing offensive or pornographic material	X			X		
Deliberately accessing or trying to access offensive or pornographic material	X	X	X	X	X	X
Breaching copyright or licensing regulations	X		X	X	X	X

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of digital/video images that they have recorded themselves or downloaded from the internet. However, staff, parents/carers and pupils need to be aware of the risks associated with publishing digital/video images on the internet. Such digital/video images may provide avenues for online bullying to take place. Digital/Video 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 academy will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm.

- Written permission from parents/carers will be obtained before any digital/video images of pupils are published on the academy website, newsletter, displays around the academy, Class Dojo, social media, academy promotional materials and in the local press. These digital/video images can still be used once the pupil has left the academy or for a limited time.
- All staff are governed by their contract of employment and the academy's Acceptable Use Policy, which covers the use of mobile phones/personal equipment for taking pictures of pupils, and where these are stored.
- Whenever a photo or video is taken/made, the member of staff taking it will check the latest permission spreadsheet before using it for any purpose
- When using digital/video images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of digital/video images. In particular they should recognise the risks attached to publishing their own digital/video images on the internet e.g. on social networking sites.
- Staff and volunteers are allowed to take digital/video images to support educational aims, but must follow academy policies concerning the sharing, distribution and publication of those digital/video images. Those digital/video images should only be taken on academy equipment, the personal equipment of staff should not be used for such purposes.
- Location Tags must not be used when taking digital/video images.
- Care should be taken when taking digital/video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the academy into disrepute.

- Digital/Video images published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such digital/video images.
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with digital/video images
- Any pupils shown in public facing materials are never identified with more than first name (and photo file names/tags do not include full names to avoid accidentally sharing them
- LAC pupils will never have digital/video images used online unless the academy has permission from the carers to do so.
- The academy will periodically invite an official photographer into academy to take portraits/photographs of individual children and/or class groups. The academy will undertake its own risk assessment in terms of the validity of the photographer/agency involved and establish what checks/vetting has been undertaken. Parents' permission is obtained before these photos are taken
- Digital/Video images are stored on a secure area on the server or on RMUnify and should not be stored on portable external hard drive devices.
- In accordance with guidance from the Information Commissioner's Office, parents/ carers are welcome to take videos and digital images of only their own children at academy 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 child protection, these digital/video images should not be published/made publicly available on social networking sites, nor should parents/carers comment on any activities involving other pupils in the digital/video images.
- Parents are reminded at each public event in academy about the importance of not sharing without permission, due to reasons of child protection (e.g. looked-after children often have restrictions for their own protection), data protection, religious or cultural reasons, or simply for reasons of personal privacy.
- Parents are not allowed to photo or video staff without their permission.
- Parents are governed by the academy's Acceptable Use Policy.
- As part of their work, pupils will have access to the use of digital cameras/iPads. Any digital/video images that they take, will be kept at the academy or on the device and the children will be taught about the need to keep these digital/video images private.
- When on visits, pupils are not allowed to take their own cameras or use cameras on phones without permission.
- Pupils are taught about how images can be manipulated in their online safety education programme and also taught to consider how to publish for a wide range of audiences which might include governors, parents or younger children
- Pupils are advised to be very careful about placing any personal photos on social media. They are taught to understand the need to maintain privacy settings so as not to make public, personal information.
- Pupils are taught that they should not post images or videos of others without their permission. We teach them about the risks associated with providing information with images (including the name of the file), that reveals the identity of others and their location. We teach them about the need to keep their data secure and what to do if they or a friend are subject to bullying or abuse.

Communications

When using communication technology the academy considers the following as good practice.

- The official academy email service is used for all academy emails.

- The official academy email service is monitored. This is for the mutual protection and privacy of all staff, pupils and parents, supporting safeguarding best-practice, protecting children against abuse, staff against potential allegations and in line with UK data protection legislation.
- Staff never use a personal/private email account (or other messaging platform) to communicate with children or parents, or to colleagues when relating to academy/child data,
- Where devices have multiple accounts for the same app, mistakes can happen, such as an email being sent from or data being uploaded to the wrong account. If this a private account is used for communication or to store data by mistake, the Headteacher should be informed immediately.
- Data protection principles will be followed at all times when it comes to all academy communications, in line with the academy Data Protection Policy.
- Users must immediately report to the Headteacher, 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.
- Users must immediately report to GBMicros any email that they think is phishing, spam or looks suspicious by its content.
- Users should know that spam, phishing and virus attachments can make emails dangerous.
- Any digital communication between staff and pupils or parents/carers (email, social media, chat, blogs, etc.) must be professional in tone and content. These communications may only take place on official academy systems. Personal email addresses, text messaging or social media must not be used for these communications.
- Appropriate behaviour is expected at all times, and the system should not be used to send inappropriate materials or language which is or could be construed as bullying, aggressive, rude, insulting, illegal or otherwise inappropriate, or which (for staff) might bring the academy into disrepute or compromise the professionalism of staff
- Emails using inappropriate language, images, malware or to adult sites will be blocked/monitored and not arrive at their intended destination (and will be dealt with according to the appropriate policy and procedure).
- Any unauthorised attempt to use a different system may be a safeguarding concern or disciplinary matter and should be notified to the DSL (if by a child) or to the Headteacher (if by a staff member).
- Users should know that email sent to an external organisation must be written carefully, (and may require authorisation), in the same way as a letter written.
- Users should know that the sending of multiple or large attachments should be limited, and may also be restricted by the provider of the service being used.
- The academy does not publish personal email addresses of pupils/staff on the academy website.
- Pupils and staff are allowed to use the email system for reasonable and not excessive periods during lessons.
- Pupils 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.

Protecting Professional Identity

The academy full Social Media Policy is included in the Appendix (page 56).

Our academy has a duty of care to provide a safe learning environment for pupils and staff. The academy 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 academy liable to the injured party. Reasonable steps to prevent predictable harm must be in place. The academy provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the academy through:

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

Academy staff should ensure that:

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

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

- A process for approval by senior leaders.
- A 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.
- Systems for reporting and dealing with abuse and misuse.
- An understanding of how incidents may be dealt with under academy disciplinary procedures.

Academy Website

The academy website is a key public-facing information portal for the academy community (both existing and prospective stakeholders) with a key reputational value.

- The Headteacher takes overall responsibility to ensure that the website content is accurate and the quality of presentation is maintained with support from the Computing lead.
- The academy website complies with the statutory DfE guidelines for publications.
- Most material is the academy's own work; where other's work is published or linked to, we credit the sources used and state clearly the author's identity or status respecting and uphold copyright law
- The point of contact on the website is the academy address, telephone number and we use a general email contact address. Home information or individual email identities will not be published.
- Digital/Video images published on the website do not have full names attached and consent is obtained.
- We do not use pupils' names when saving digital/video images in the file names or in the tags when publishing to the academy website.

- We expect teachers using academy approved blogs or wikis to password protect them and run from the academy website.

Class Dojo Staff

- Staff will message parents in working hours.
- Should staff receive any messages which they find inappropriate, they will report to SLT as soon as possible.
- Staff should not share any personal information.
- Any messages which refer to absence, sickness or complaints should be directed to the academy office.
- Any messages which refer to progress will be discussed face-to-face or over the phone.
- In photos, children will be dressed appropriately and will have photo consent from their parents/carers.
- Staff should be aware of who/what is in the background of a photo/video.
- Staff will think about copyright when posting or approving user content.
- All communication must be appropriate and related to academy matters.
- Always use the same professional language and tone as you would in person. Staff should use academy devices over personal devices wherever possible.
- Staff should not be communicating with pupils unless it is for the safety of the pupil.
- Staff will not use the site in any way that is harmful to minors.

Parents

- Parents/Carers should be aware that an immediate response to a message cannot be expected as the main priority of the staff is to teach. A response will be given as soon as possible during working hours.
- Any matters about absence, sickness, academy dinners or complaints should go to the academy office via telephone or in person.
  Any queries about progress should be directed to the class teacher directly either face-to-face or over the phone.
- Parents/Carers should not copy, reproduce, modify or distribute any text or images/photos from Class Dojo without permission from the class teacher.
- Parents/Carers should be aware of what is in the background of a photo/video.

- Photos of children sent to the class teacher should not be taken in bedrooms and your child should be appropriately dressed.
- Parents/Carers will not post unauthorised commercial communication.
- Parents/Carers will think about copyright when posting content.
- Parents/Carers will not use another person's login details or access an account belonging to someone else.
- All communication with the class teacher must be polite, appropriate and related to academy matters.
- Parents/Carers will not do anything that will impair the workings or appearance of Class Dojo.
- Parents/Carers will not use the site in any way that is harmful to minors.

Pupils

- Pupils should not be using Class Dojo to communicate with their class teacher.

Cloud-Based Technologies

- Uploading of information on the academy's RMUnify is shared between different staff members according to their responsibilities.
- Digital/Video images uploaded to the academy's systems will only be accessible by members of the academy community.

School YouTube Channel

- Videos can only be uploaded to the academy YouTube channel by a member of SLT who will check them first.
- Uploaded videos must have the appropriate child settings applied.
- No child without parental consent should be included in a video.
- Staff/pupils should be appropriately dressed.
- Staff should always consider what can be seen in the background of the video.
- Staff should always consider the noises in the background.

YouTube Videos

- Staff should always watch the video first to ensure the content is safe.
- Staff should always ensure that the children do not watch adverts.
- Staff should always ensure that the children do not see links to inappropriate content.
- Children should never be allowed to search for videos on a staff member's laptop or be left alone watching a video.
- The academy filters deny access to YouTube on pupil logins.

Live Streaming/Video Conferencing on Site

- Facebook Live, Instagram Live and YouTube Live are not used to live stream in the academy. Zoom/Microsoft Teams may be used but permission needs to be sought from the SLT.
- The appropriate filters need to be in place to keep children safe.
- Permission is sought from parents/carers.
- All pupils are supervised by a member of staff at all times.
- Approval from the Headteacher/SLT is sought prior to all video conferences/live streaming within the academy.
- The academy equipment is not set to auto-answer and is only switched on for scheduled and approved video conferences/live streams.

- No part of any video conference/live stream is recorded in any medium without the written consent of those taking part.
- Staff are aware of what is in the background that people can see or hear.
- All members of staff have a good knowledge of what they are streaming before they start.
- Misuse of video conferencing/live streaming by any member of the academy community will result in sanctions.
- Participants in conferences offered by 3rd party organisations may not be DBS checked so pupils must be supervised by a staff member at all times.
- Conference/Streaming supervisors need to be familiar with how to use the equipment, particularly how to end a call if at any point any person taking part becomes unhappy with the content of the video conference/live stream.
- Staff should use academy devices over personal devices wherever possible.

Live Streaming/ Video Conferencing from Staff Homes

- Facebook Live, Instagram Live and YouTube Live are not used to live stream in the academy. Microsoft Teams and Zoom may be used but permission needs to be sought from the Computing Leader/SLT.
- Staff should be appropriately dressed.
- Staff should always consider what can be seen in the background.
- Staff should always consider the noises in the background.
- The appropriate filters/settings need to be in place to keep children safe these must be checked by SLT.
- All members of staff have a good knowledge of what they are live streaming/video conferencing before they start.
- The academy equipment is not set to auto-answer and is only switched on for scheduled and approved conferences.
- No part of any video conference/live stream is recorded in any medium without the written consent of those taking part and approved by SLT.
- Participants in conferences offered by 3rd party organisations may not be DBS checked so pupils must be supervised by a staff member at all times.
- Staff should use academy devices over personal devices wherever possible.
- Conference/Streaming supervisors need to be familiar with how to use the equipment, particularly how to end a call if at any point any person taking part becomes unhappy with the content of the video conference/live stream.

Remote Learning

Where children are being asked to learn online at home Zoom will be the preferred platform. Parents will be required to sign the Pupil Acceptable Use Policy (AUP) for Live Lessons using Zoom and staff will follow the Pupil Acceptable Use Policy (AUP) for Live Lessons using Zoom. These are both included in the Appendix Page 53 - 54

The NSPCC and PSHE Association also provide helpful advice:

• NSPCC Learning - Undertaking remote teaching safely during school closures • PSHE - PSHE Association coronavirus hub

Webcams

- We do not use publicly accessible webcams in the academy.

- Webcams in the academy are only ever used for specific learning purposes.
- Misuse of the webcam by any member of the academy community will result in sanctions.

Off Boarding and On Boarding Staff

This is brought to the attention of Jenny Bray (Trust IT Manager) and GBMicros (Academy Network Manager) by Nicole Lang – Computing

New Staff to the Academy

1. Read and sign Acceptable Use Policy. Nicole Lang – Computing Lead
2. Read and sign they have read Online Safety Policy. Nicole Lang – Computing Lead
3. Give laptop and record serial number with GBMicros. Nicole Lang – Computing Lead
4. Generate login for laptop and access to the academy server. GBMIcros
5. Generate login for RMunify and email address. GBMIcros
6. Give access to the correct email groups – eg TCIA All Staff.
7. Generate a printer code. GBMIcros
8. Training given on how to use systems in school

Staff Leaving the Academy

1. Collect in Laptop and check against serial number. Nicole Lang – Computing Lead
2. Remove access for laptop and the academy server. GBMIcros
3. Remove access for RMunify and email address. GBMIcros
4. Remove access for email groups
5. Remove access for printer code. GBMIcros

Asset Disposal

All redundant equipment will be disposed of through an authorised agency. All redundant equipment that may have held personal data will have the storage media forensically wiped. Alternatively, if the storage media has failed, it will be physically destroyed. The academy will only use authorised companies who will supply a written guarantee that this will happen. Disposal of any equipment will conform to The Waste Electrical and Electronic Equipment Regulations 2006 and/or The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007. Further information can be found on the Environment Agency website.