# Online Safety Policy

## Including: Mobile Technologies and Academy Technical Security

## Written in accordance with the

## Social Media Policy and

## Data Acceptable Use Policies

## Cybersecurity Policy

## September 2024

Review: September 2025

**We Grow Greatness**

**Online Safety Lead – Beth Hunter**

**Signed _____________________ Sharon Wood**
**Headteacher**

**Signed _____________________ Michelle Sills**
**Chair of Governors**

## 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’ 2024 (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.

## 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:<br>Headteacher: Sharon Wood<br>Online Safety Governor: Lynne Thompson<br>Filtering and Monitoring Governor: Lynne Thompson<br>Safeguarding Governor: Michelle Sills | |
| 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:<br>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 – Net Sweeper and Jamf Safe Internet on iPads.
- 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, Sharon Wood 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)
- Included in all staff's safeguarding folder
- Integral to safeguarding updates and training for all staff (especially in September refreshers)
- Clearly reflected in the Data Acceptable Use Policies (AUPs) for staff, volunteers, contractors, governors, pupils and parents/carers
- Data Acceptable Use Policy for parents/carers and pupils are shared and signed online
- Data Acceptable Use Policy discussed with pupils and signed at the start of each year
- Data Acceptable Use Policy to be issued to whole academy community on entry to the academy
- Data 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 Academy Business Leader, 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 WhatsApp group chats which leads to the pupils making hurtful and inappropriate comments to each other.

- The use of TikTok and the algorithm it uses to steer pupils towards looking at inappropriate links such as body image or using homophobic language.

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 2024' 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 'self-generated' 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 2024/2025

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: Anti-social-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.

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 Junior 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)

## The main areas of risk for our academy community can be categorised into four areas of risk:

### 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 semi-nudes 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 Junior 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 Data Acceptable Use Policy in conjunction with this policy, the Safeguarding Policy, the code of 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 and avoiding 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. Staff should reinforce pupil's 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 Data 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. Lynne Thompson, 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 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.
- Ensure all stakeholders are informed about the current filtering and monitoring.

**Headteacher**

As all staff, plus:

**Key responsibilities:**

- 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**

As all staff plus:

**Key responsibilities**

- 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. Data 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 (e.g. by use of the updated UKCIS framework 'Education for a Connected World – 2020 edition') and beyond, in wider academy life.
- 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**
**Key responsibilities:**
As all staff, plus:

- 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**
**Key responsibilities:**
As all staff, plus:

- Oversee delivery of the online safety element of the Computing curriculum in accordance with the national curriculum.
- 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.
- Work closely with the PSHRE lead to avoid overlap but ensure a complementary whole-academy approach.

- Work closely with the DSL and all other staff to ensure an understanding of the issues, approaches and messaging within Computing.
- Collaborate with technical staff and others responsible for ICT use in the academy to ensure a common and consistent approach, in line with acceptable-use agreements.

**Subject Leaders**
**Key responsibilities:**
As all staff, plus:

- 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 staff**

**Key responsibilities:**
As all staff, plus:

- 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, Jamf Safe Internet on iPads 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. (see Appropriate Filtering and Monitoring section)

- Maintain devices with software, security and antivirus updates. (see Technical Support section)
- Ensure the Cybersecurity Policy is up to date, easy to follow and practicable.

**Data Protection Officer (DPO)**
**Key responsibilities:**

- 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 2024, "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.

**Volunteers and contractors (including tutors)**
**Key responsibilities:**

- Read, understand, sign and adhere to an Data 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**
**Key responsibilities:**

- Read, understand, sign and adhere to the student/pupil Data Acceptable Use Policy.
- Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- 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.
- Take care of all academy provided devices whether used on the academy site or at home.
- Use provided apps like Showbie, Purple Mash and TTRockstars respectfully never causing harm or upset to anyone else and should never access anyone else's account.

**Pupil Online Safety Leaders**
**Key responsibilities:**

- Conducting assemblies to the whole academy about current online safety issues.
- Offering child-to-child support about staying safe online.
- Talking to parents about current online safety issues.
- Writing online safety help tips on the academy newsletters.
- Interviewing pupils to gain pupil voice about current online safety issues.
- Helping to write the Pupil Data Acceptable Use Agreement and Online Safety Policy.

**Parents/Carers**
**Key responsibilities:**

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

**External groups including the parent association**
**Key responsibilities:**

- Any external individual/organisation will sign the Data Acceptable Use Policy prior to using technology or the internet within the academy.
- Support the academy in promoting online safety and data protection.
- Model safe, responsible, respectful and positive behaviours in their own use of technology, including on social media: not sharing other's images or details without permission and refraining from posting negative, threatening or violent comments about others, including the academy staff, volunteers, governors, contractors, pupils or other parents/carers.

## 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. We use Jigsaw, Education in a Connected World, Project Evolve and BBC Own It resources to teach eight strands of online safety. They are: Self-Image and Identity, Online Relationships, Online Reputation, Online Bullying, Managing Online Information, Health, Well-being and Lifestyle, Privacy and Security and Copyright and Ownership. 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
- Citizenship

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 2024.

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 2024 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
- Data 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

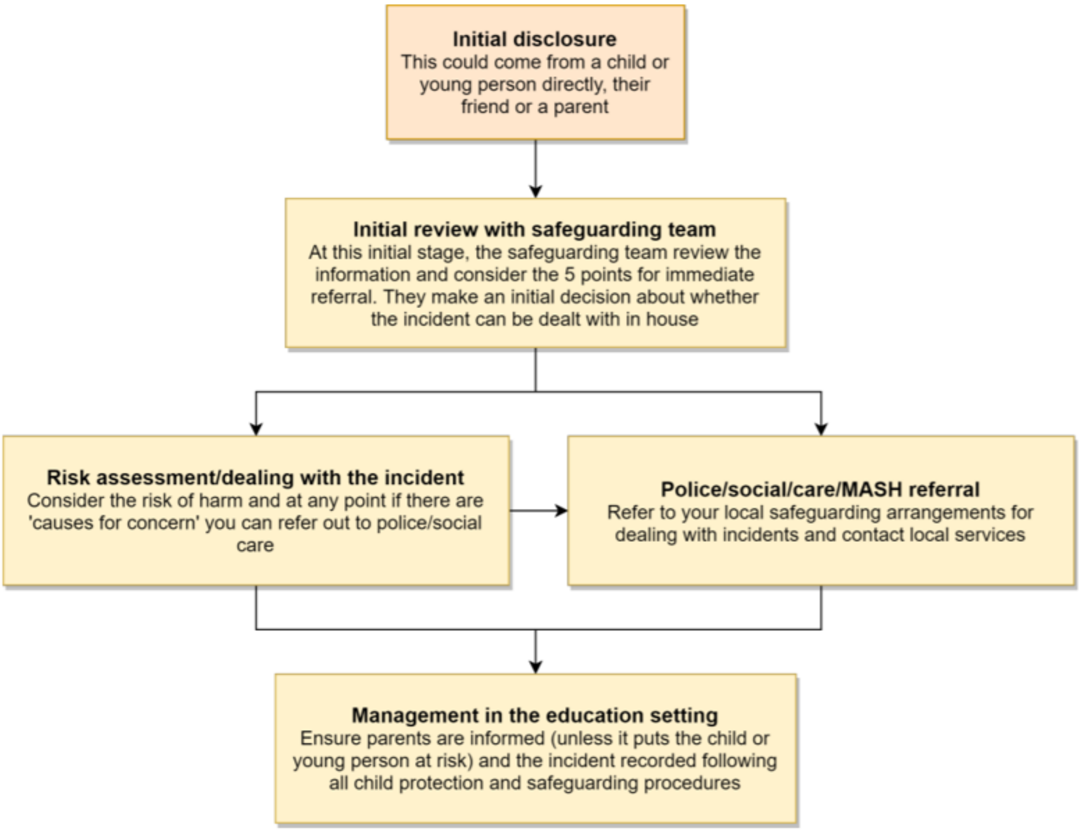
**What to do if an incident involving 'sharing nudes or semi-nudes' comes to your attention:**

- 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-with-children-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.

Guidance is also in the Data Acceptable Use Policy.



**Initial disclosure**
This could come from a child or young person directly, their friend or a parent

**Initial review with safeguarding team**
At this initial stage, the safeguarding team review the information and consider the 5 points for immediate referral. They make an initial decision about whether the incident can be dealt with in house

**Risk assessment/dealing with the incident**
Consider the risk of harm and at any point if there are 'causes for concern' you can refer out to police/social care

**Police/social/care/MASH referral**
Refer to your local safeguarding arrangements for dealing with incidents and contact local services

**Management in the education setting**
Ensure parents are informed (unless it puts the child or young person at risk) and the incident recorded following all child protection and safeguarding procedures

***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 non-consensual 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-on-child 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 'cyber-enabled' (crimes that can happen off-line but are enabled at scale and at speed on-line) or 'cyber dependent' (crimes that can be committed only by using a computer). Cyber-dependent crimes include:

• Unauthorised access to computers (illegal 'hacking'), for example accessing 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 2024, "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/Logins

The Carlton Junior 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. Logs of student passwords are retained in a secure location in each primary school to assist students should they forget their passwords.

## Technical Support – infrastructure/equipment

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 systems, files and devices which are managed by GBMicros.
- Devices and systems have an appropriate level of encryption.
- 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 Data Acceptable Use Agreement.
- Remote management tools are used by staff to control devices 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 devices are protected by software, security and anti-virus updates.
- 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 as outlined in the Data Acceptable Use Policy.

**iPads**

Technical support for iPads is managed by KRCS.

- An agreed procedure is in place to remove Safari, the camera and the Showbie App on pupil iPads before iPads are taken home.
- Apps can only be installed by KRCS.
- Apps to be installed have to be approved by SLT or the Computing Lead before being installed.

## Remote Access

Refer to Data Acceptable Use Policy.

## 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

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

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. There are regular training reminders in the light of the annual review and regular checks that will be carried out.

At The Carlton Junior Academy:

- Web filtering is provided by Schools Broadband and is called Netsweeper. Jamf Safe Internet is used to filter the iPads.
- The filtering occurs both on the academy site and for devices used in the home.
- Internet filtering/monitoring ensures that children are safe from harmful content when accessing the internet.
- All internet usage is recorded and metadata retained.
- Emails are filtered using Microsoft defender which ensures that malware and viruses are blocked from delivery.
- Microsoft filter spam and junk using their own internal systems and will remove and quarantine emails.
- 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.
- Changes can be made by Beth Hunter, Sharon Wood, GBMicros (Schools Broadband) and KRCS (Jamf Safe Internet)
- Overall responsibility is held by the DSL
- Technical support and advice, setup and configuration are from Beth, GBMicros (Schools Broadband) and KRCS (Jamf Safe Interne)t
- Regular checks are made half termly by Sharon Wood, Beth Hunter, GBMicros (Schools Broadband) and KRCS (Jamf Safe Internet) to review the effectiveness of the filtering and monitoring systems in place.
- An annual review is carried out during our Cybersecurity review.
- SENSO Alerting Software is loaded on all Window devices which monitors all activity on devices and alerts Sharon Wood, the safeguarding team and the office, if there has been a violation.

## Personal devices including wearable technology and bring your own device (BYOD)

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. Digital images and video should never be taken on a personal digital device as outlined in the Digital images and video section of this document. 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.
- Staff must use phones provided by the school where possible to conduct all work-related business where possible. 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 personal phone number.
- Staff must never give their personal number to parents or pupils.
- 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 on the academy site. They should ask permission before taking any digital images or videos. When at academy events certain procedures are in place, please refer to the Digital images and video section of this document. 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 as well as appropriate personal use.
- All and any usage of devices and/or systems and platforms may be tracked.

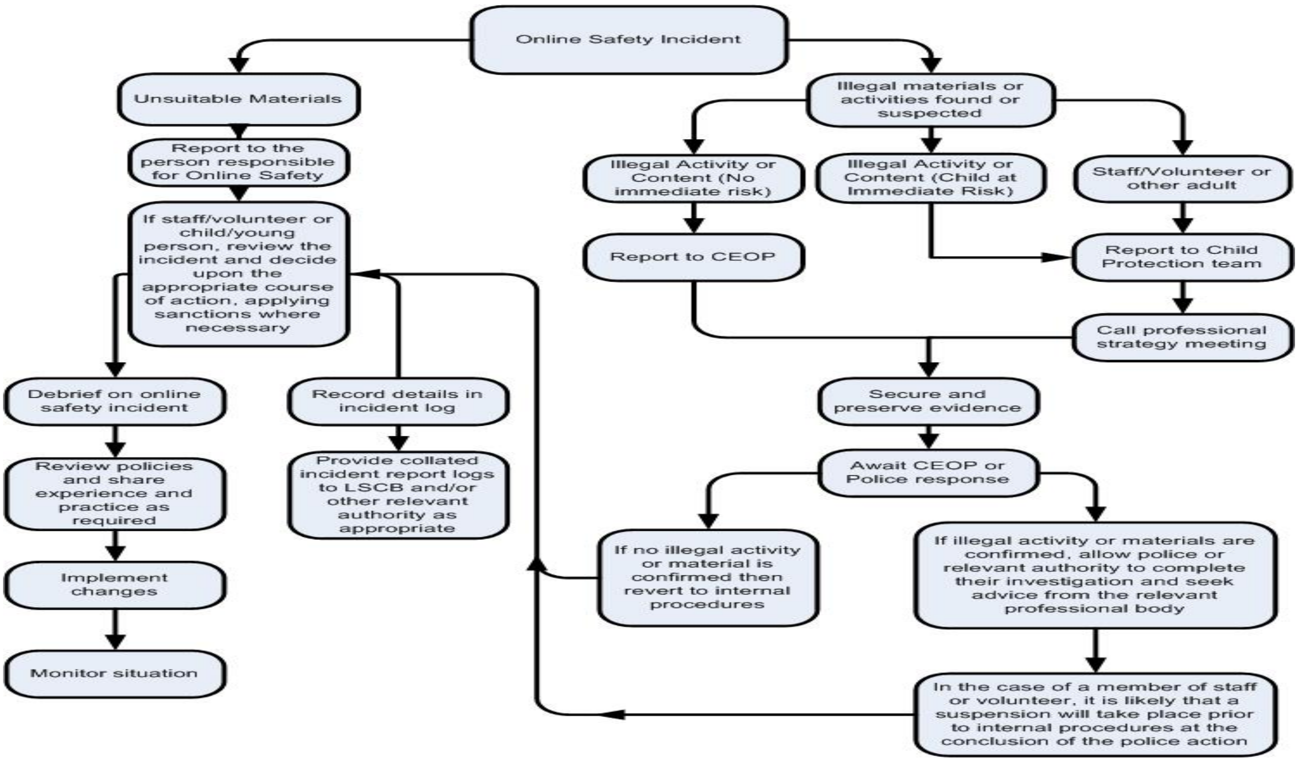
## Misuse of academy technology (devices, systems, networks or platforms)

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 Data 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.


Online Safety Incident
Unsuitable Materials
Report to the person responsible for Online Safety
If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary
Debrief on online safety incident
Review policies and share experience and practice as required
Implement changes
Monitor situation
Record details in incident log
Provide collated incident report logs to LSCB and/or other relevant authority as appropriate
Illegal materials or activities found or suspected
Illegal Activity or Content (No immediate risk)
Illegal Activity or Content (Child at Immediate Risk)
Staff/Volunteer or other adult
Report to CEOP
Report to Child Protection team
Call professional strategy meeting
Secure and preserve evidence
Await CEOP or Police response
If no illegal activity or material is confirmed then revert to internal procedures
If illegal activity or materials are confirmed, allow police or relevant authority to complete their investigation and seek advice from the relevant professional body
In the case of a member of staff or volunteer, it is likely that a suspension will take place prior to internal procedures at the conclusion of the police action

## 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 Data 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). They must ensure no other children are in these videos or digital images. 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 Data 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 iPads are taken home cameras are disabled.
- 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.0
- 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.

## 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 site is managed by CODA Education.

- 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.

## Communications

### Email

The school provides each member of staff with a work email address. This email account should be used for work purposes only. For appropriate use of emails please also refer to the Data Acceptable Use Policy.

### Social Media

The academy uses X (formerly Twitter) to showcase achievements and events. This is not used to communicate individually with anyone. For further information please refer to The Social Media Policy and Data Acceptable Use Policy.

### 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/One Drive/Showbie 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 Data Acceptable Use Policy (AUP) for Live Lessons using Zoom and staff will follow the Pupil Data Acceptable Use Policy (AUP) for Live Lessons using Zoom. These are both included in the Appendix

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.

## Choosing Online Tutors

The academy does not use Tutoring online. Should it be used in the future, it will be considered as a regulated activity and the requirements of Keeping Children Safe in Education (KCSIE 2020) and Safer Recruitment followed.

## Games Machines

The academy does not use Games machines.

## Off Boarding and On Boarding Staff

This is brought to the attention of Jenny Bray (Trust IT Manager) and GBMicros (Academy Network Manager) by Beth Hunter - Computing Lead or Angela Cooke - Administrative Officer.

**New Staff to the Academy**

1. Read and sign Data Acceptable Use Policy. Beth Hunter – Computing Lead
2. Read and sign they have read Online Safety Policy. Beth Hunter – Computing Lead
3. Give laptop and record serial number with GBMicros. Beth Hunter – Computing Lead
4. Generate login for laptop and access to the academy server. GBMicros info@gbmicros.co.uk
5. Generate login for RMunify and email address. GBMicros info@gbmicros.co.uk
6. Give access to the correct email groups – eg TJCA All Staff. IT Manager, The Redhill Academy Email: j.bray@theredhillacademy.org.uk
7. Generate a printer code. GBMicros info@gbmicros.co.uk
8. Training is given on how to use the systems in the academy, how to encrypt emails and how to use 141 on your own phone. Beth Hunter – Computing Lead

**Staff Leaving the Academy**

1. Collect in Laptop and check against serial number. Beth Hunter – Computing Lead
2. Remove access for laptop and the academy server. GBMicros info@gbmicros.co.uk
3. Remove access for RMunify and email address. GBMicros info@gbmicros.co.uk
4. Remove access for email groups – eg TJCA All Staff. IT Manager, The Redhill Academy Email: j.bray@theredhillacademy.org.uk
5. Remove access for printer code. GBMicros info@gbmicros.co.uk
6. Remove photo on the academy website. Angela Cooke – Clerical Assistant

## 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.

## Appendices

## iPad Acceptable Use Policy

Date created 19/12/2023
Date of review 19/12/2024
Committee Sharon Wood (Head teacher), Beth Hunter (Computing Lead), Annabel Simmons (iPad Lead), KRCS and GB Micros.

### Contents:

### iPad Acceptable Use Policy:

The policies, procedures and information within this document apply to all iPad devices used in school and at home. Teachers and other school staff may also set additional requirements for use within their classroom. Users must use protective covers/cases for their iPads.

Users in breach of the Acceptable Use Policy may be subject to but not limited to: disciplinary and charge action, confiscation, removal of content or referral to external agencies in the event of illegal activity.

The Carlton Junior Academy is not responsible for: the financial or other loss of any personal files that may be deleted from an iPad.

### Software and Apps:

- Periodic checks will be made to ensure the iPads are being kept up to date and are in a useable state.
- Upgrade versions of apps are available from time to time.

### Charging the iPad

- If you need to charge your iPad at home, only authorised Apple iPad chargers suitable for the provided iPad must be used.
- iPads can be turned off when they are not required to save battery power during the school day or at home.
- Pupils will only use the designated charging stations which are named for each child.
- There will be charging banks in each classroom so iPads can be charged at appropriate times during the day.

**Additional Responsibilities for Pupils:**

If an iPad is left at home or is not charged, the user remains responsible for completing all school work as if they had use of their iPad. Malfunctions or technical issues are not acceptable excuses for failing to complete school work, unless there is no other means of completion. Pupils must not use their iPad in school corridors, on their journeys to and from school or outside of school buildings (unless with the teacher's permission).

When completing homework, iPads will be locked so pupils can only access the appropriate apps at home. Teachers will let parents/carers know which app to use for which week. There will be a timer on the iPads so pupils are using them at an appropriate time. When using the iPads at home, parents and carers must ensure iPads are not used in bedrooms.

**Safeguarding and Maintaining as an Educational Tool:**

The whereabouts of the iPad will be known at all times, and will be tracked on all devices.

It is the user's responsibility to keep their iPads safe and secure. iPads belonging to other users are not to be tampered or interfered with in any manner. All iPads will have name labels so there is no confusion. If an iPad is found unattended, it should be given to the nearest member of staff.

**Lost, Damaged or Stolen iPad:**

If your child's iPad is lost, stolen or damaged, a school member of staff must be notified immediately, with a report on how it was lost, stolen or damaged. Parents will be required to compensate school to replace the iPad - (iPads are rarely subject to physical damage if cases are not removed). IPads must remain in school's protective casing at all times. IPads are labelled with pupil's P numbers, first name and last initial.

**Cameras:**

Photographs may only be taken when authorised by a member of staff in relation to: school, work or homework. The camera must not be used to take inappropriate or explicit photographs or videos, nor will it be used to embarrass anyone in any way, or violate any of the school's policies, which are available on our school's website. The iPad is subject to routine monitoring.

**Misuse of Password, Codes or other Unauthorised Access:**

The authorised user for the iPad is the pupil of The Carlton Junior Academy. The iPad must be used for educational purposes, or purposes set by the class teacher. Any user caught trying to gain access to another user's device, files or data will be subject to disciplinary action. The iPad Lead will have regular contact with KCRS and GB Micros to seek advice when/if needed.

**Parent/Carer/Pupil Pledge and Commitment for iPad Usage:**

The school has developed a set of rules to help keep pupils safe whilst using technology e.g. iPads and the internet. Pupils will be reminded of their responsibilities whilst using technology. These rules will be kept under constant review and amended as required. Additional clauses may come into effect at any time, but will be communicated. The Acceptable Use Policy must be signed and returned to the school via Google Forms before a pupil can take their iPad home.

**The Following Rules Apply to all Pupils:**

- Treat my iPad with the upmost care and respect.
- Know my iPad is to be used for homework and educational purposes only.
- Use my iPad to complete my homework task and ask for help from my parent/carer if and when needed.
- Not to download apps, or make purchases on the iPad.
- Keep the stylus attached to my iPad when I'm not using it and keep the protective case on at all times.
- Never drop or place heavy items on top of my iPad.
- Keep food and drink away from my iPad.
- Only use my iPad in supervised areas at home and know it must not be taken anywhere else.

**Online Safety:**

- If asked to click on something (such as 'accept'), check with an adult first.
- Report anything I am unsure of to Mrs Wood, Miss Simmons, Mrs de Gilbert, Miss Hodgson or Mrs Hunter at school, after showing an adult at home.

- Support the school's Online Safety Policy (available on our website) and not deliberately upload/download any images, videos, sounds or text that could upset any member of the school community.
- Only use my log in and password when using online learning environments and keep them private.
- Never share any images or digital media of people on the internet.
- Understand that the iPad is monitored and filtered.

**Parent/Carer Commitment:**

✓ Monitor and oversee your child's iPad use within your home.
✓ Please do not allow your child to use the iPad unsupervised or in the bedroom.
✓ Help your child with homework set on the iPad.
✓ Do not leave the iPad in an unattended vehicle or a place where it can be stolen.
✓ Do not use the iPad for your own personal use.
✓ Understand that school cannot be held responsible for the content of material accessed at home. However, school will take the necessary measures to work with you to keep your child safe.
✓ Understand that iPads are tracked and monitored and filtered by school.
✓ Agree not to undertake repairs or modifications on the iPad.

**Your Commitment:**

I understand that if the iPad is damaged or lost, I will need to compensate the school to replace the iPad. The iPads cannot be repaired.
I have read and understood the iPad Acceptable Use Policy document, as well as this declaration. I give my permission to my son/daughter to use the iPad as outlined in this policy.
The iPad remains the property of The Carlton Junior Academy and must be returned when requested.

**Sanctions:**

That school has the right to take action with me if involved in incidents or inappropriate behaviour that are covered in this agreement when outside of school and where they involve my membership of the school community (examples: online bullying or use of personal information).
1. A letter home informing parent/guardian/carer of the nature and the breach of rules.
2. The Redhill Trust and/or police informed.
3. Suspension of iPad
4. Cost of damaged or lost items

**School Responsibilities:**

● We will manage pupil devices at all times.
● We will update apps when needed.
● We will provide every child with an iPad, iPad pen and case to help support their learning.
● We will ensure children with additional needs have access to tools to support their learning.
● We will maintain/repair iPads if there are problems resulting from use in school.
● We will set suitable filters to protect pupil online searches.
● We will ensure the iPad will run through secure filters at school and at home.
● We will use search reports will inform the teaching of online safety.
● We will teach Digital Citizenship to help children understand how to stay safe online (age appropriate).
● We will celebrate Safer Internet Day and regularly teach about Online Safety.
● We will have assemblies focussing on online safety.
● We will support parents if they wish to learn more about devices, their use and online safety.

**Home Use:**

● Pupils are allowed to use their iPads outside of School with parent/carer consent. The iPad can connect to other wireless networks to assist them with their homework. It is the responsibility of the parent/carer to monitor and oversee iPad use within the home setting and the pupil must be supervised by a responsible adult at all times.

● Photographs may only be taken on the iPad when authorised by a member of staff in relation to School homework. The iPad cameras are not to be used at any other time to save space and prevent misuse of the iPad.

## Redhill Academy Trust Safeguarding protocols during enforced partial closure of academies.

### Online safety

It is likely that children will be using the internet and engaging with social media far more during this time. Our staff are aware of the signs of cyberbullying and other online risks and for children in academy our filtering and monitoring software remains in use during this time to safeguard and support children.

Where staff are interacting with children online they will continue to follow our IT Acceptable Use policy. Staff who interact with children online will continue to look out for signs a child may be at risk. If a staff member is concerned about a child, that staff member will report that concern to the DSL or to a deputy DSL as they would with all safeguarding concerns.   Any contact will be through the parental email address, not a child's personal email address.

Parents will be advised of different links that are available to them to support them in helping to keep their child safe online:

- Thinkyouknow (advice from the National Crime Agency to stay safe online)
- Internet matters
- Parentinfo
- LGfL
- Net-aware (advice from the NSPCC)

**Pupil Acceptable Use Policy (AUP) for Live Lessons using Zoom**

Parents/Carers must ensure that they read this policy alongside their child before using Zoom to access live lessons.
This AUP is essential for managing and sustaining the integrity and legality of The Carlton Junior Academy network and computing resources. Please read and send a message to the class teacher via Class Dojo, to let them know that you agree to the following protocols. These will help to protect you and your child.

- Do not create or use an existing Zoom account for your child. Always join a meeting by following the link the teacher has sent. We will be using our academy account for this.
- Make sure the Meeting ID and Password is from our academy Class Dojo platform.
- When joining a live lesson make sure that the name that appears on the screen for your child is their first name and the initial of their surname, so that the teacher can let them into the lesson.
- For your child's safety we may record the lesson. The recordings are kept for 6 months and no-one is permitted to view them without good reason and only with permission from the Headteacher.
- Children and parents are not permitted to start a meeting, make screen grabs, take photos of or record any of the live lessons and share them.
- Children are not permitted to call, chat, set up private groups between each other.
- Ideally, your child should be somewhere in their home away from others so that they can concentrate and so that siblings or other household members will not inadvertently broadcast to the class.
- Children should not be in a room on their own with a closed door and an adult should frequently check in on them.
- Parents should think about what is in the background and if possible blur the background for their child if in a virtual lesson which involves a camera.
- Children should be fully dressed for live meetings (no nightwear) and wear their academy uniform top.
- Microphones should be muted, unless directed by the teacher to turn them on.
- Your child can use the hands up tool (if available) if they want to talk.
- When written chat is enabled it should be appropriate and polite and your child should never upload anything into this chat.
- Your child is expected to follow the usual high standards of behaviour as they would in academy.
- Children/parents must hang up at the end of the lesson once instructed to do so. The teacher must be the last person in the meeting to hang up.
- Children should not respond to contact requests made from someone they don't know during the live session. They must report any such requests to the class teacher.
- Teaching staff reserve the right to remove a pupil from the meeting if the above rules are not adhered to and appropriate sanctions will be taken.
- We aim to make sure that there are two staff members on the video call.
- There should be no inappropriate content on any of our video calls. Please contact the academy if you are concerned about any of the content of the video call.

This runs alongside the academy ICT Acceptable Use Policy and Online Safety Policy.

## The Carlton Junior Academy Protocols for live teaching with Zoom

### Introduction

These protocols aim to ensure that live lessons with pupils are safe, secure and continue to model the high standards set by our academy with our pupils. This is guidance for running live lessons over Zoom and how to do this safely and best engage the pupils.

**Parental consent is being sought as we are recording the sessions to safeguard you as a teacher. The recordings of the live lessons can't be shared with parents/carers. They are to be downloaded to the agreed area on the server. The recordings are kept for 6 months and no-one is permitted to view them without seeking permission from the Headteacher.**

### Principles of live teaching

- Adhere to the Academy Staff Code of Conduct and Behaviour Policy re: professional attire, language etc.
- Treat a live virtual classroom just as you would a classroom at academy.
- Use the video facility if you are comfortable to do so.
- Mute participants to reduce background noise (this applies mainly to your participants).
- Ensure you sit in a well-lit room.
- Be mindful of what is behind you. If possible have a solid wall behind you, not a mirror or blur/turn on a virtual background.
- Do not post pictures of your virtual class on social media or elsewhere online.
- Inform DSL if you have any safeguarding concerns.
- Inform SLT if any issues occur during your live lesson.

### Using Zoom

- Always use your academy Zoom account and ensure the settings are the same as stated in the help video.
- The title of Zoom meetings will include the lesson and year group.
- Password-protect the meeting.
- Post the Meeting ID and Passcode to the lesson in advance via Class Dojo. **Do not share the link.**
- Do not schedule a meeting as a recurring meeting as it will use the same Meeting ID and Passcode.
- Use a random meeting ID for each lesson (generate automatically) – this is best practice, so the ID can't be shared multiple times.
- Ensure that you are on time to start your live lesson.
- Factor in approximately 5 minutes for pupils to enter the session. Lock Meetings once they have begun, so that no one else can enter.
- Make a note of who attends each live lesson and follow-up non-attendance.
- Teachers will ensure that the video settings for the children are off when joining. The teacher will be in charge of putting the cameras on and off for each individual child.
- Consider timings of live lessons to avoid clashes for siblings.
- Ensure the child's screen name is their first name and the initial of their surname, not their parent's name or the name of the device they are using.
- Parents can join on computers, iPads, tablets and phones.
- Teachers will have control over the screen sharing facility.
- The Waiting Room feature will be used to protect our Zoom virtual classroom and keep out those who aren't supposed to be there. They will be allowed access one-by-one to the virtual classroom.

- The chat facility (typed comments) will be controlled by the host/teacher. It can be turned off for all pupils.
- Teachers will remove any unknown participants from the lesson if necessary and appropriate actions will be taken to report incidents to SLT.
- Children not following the behaviour code can be removed from the live lesson. This will be followed-up with parents.
- Children cannot join the live lesson before the teacher joins and will see a pop-up that says, "The meeting is waiting for the host to join."
- Teachers will disable participant annotation in the screen sharing controls to prevent children from annotating on a shared screen and disrupting the live lesson.
- Teachers will always exit the "live meeting for all" at the end and be the last person to leave.
- Teachers will encourage an adult to be within 'hearing' distance during the child's live lesson.
- We will aim to have two members of staff present during the live lesson – one to deliver and one to monitor the chat if turned on and pupils in the lesson.
- Children at academy will be able to access live lessons.

**Additionally, teachers have a couple of in-meeting options to control your virtual classroom:**

- Disable video: Turn off a pupil's video to block distracting content or inappropriate gestures during class is in session.
- Mute pupils: Mute/unmute individual or all children. Live lessons will be muted upon Entry.
- Attendee on-hold: An alternative to removing a user, you can momentarily disable their audio/video connections. Click on the attendee's video thumbnail and select Start Attendee On-Hold to activate.
- Recording meetings – We will remind children of the protocols and not to share personal information at the start of live lessons. Once recorded, lessons are to be downloaded to the agreed area on the server. The recordings are kept for 6 months and no-one is permitted to view them without seeking permission from the Headteacher.
- Security Icon in Toolbar: Visible only to hosts and co-hosts of Zoom Meetings, the Security button provides easy access to several existing Zoom security features, as well as a new option to turn on the Waiting Room in-meeting. This button allows us to remove participants, lock the meeting, and decide if we want to allow our participants to screen share, chat, rename themselves, and annotate on shared content.

**Our first and ongoing virtual lessons**

- We will spend some time at the beginning checking that pupils understand their audio and video. This may be through a quick game at the start of the call!
- We will discuss online etiquette and expectations of the pupils in their first virtual class and periodically revisit this topic.
- We will take time to promote questions, comments, and reactions from the class. We will show them how muting and unmuting works and support them with asking questions or sharing comments aloud. Microphones should be muted, unless directed by the teacher to turn them on. The child can use the hands up tool if they want to talk (if available on their device).

**Most importantly, we are aiming to have fun with this new technology, engage in social interaction virtually, and keep children learning.**

**Record of Reviewing Devices or Deletion of Data/Files**

Person using device:............................................................................................

Date: ............................................................................................................

Reason for investigation:............................................................................................................................................

....................................................................................................................................................................................

.......................................................................................

Details of first reviewing person

Name: ..............................................................

Position: ..............................................................

Signature: ..............................................................

Details of second reviewing person

Name: ..............................................................

Position: ..............................................................

Signature: ..............................................................

| Device | Reason for concern |
|---|---|
| | |
| | |
| | |

Reporting Log for Online Incidents

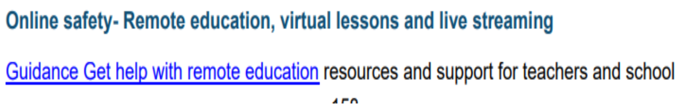
Group: ................................................................................

| Date | Time | Incident | Action Taken | | Incident Reported By | Signature |
|---|---|---|---|---|---|---|
| | | | What? | By Whom? | | |
| | | | | | | |

Reporting Log for Filtering Incidents

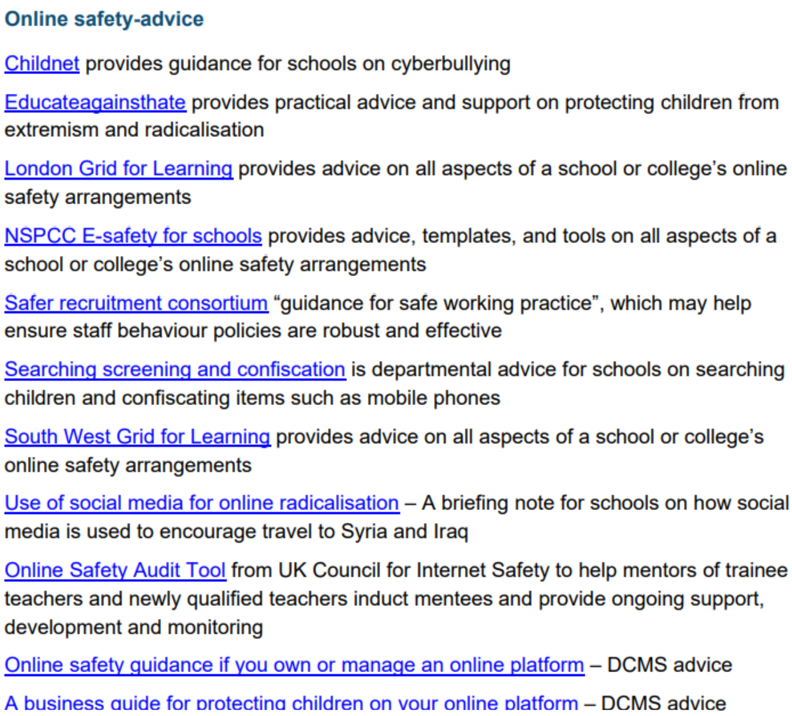
Group: ..............................................................................

| Date | Time | Incident | Action Taken | | Incident Reported By | Signature |
|---|---|---|---|---|---|---|
| | | | What? | By Whom? | | |
| | | | | | | |



## Online safety- Remote education, virtual lessons and live streaming

Guidance Get help with remote education resources and support for teachers and school



## Online safety-advice

Childnet provides guidance for schools on cyberbullying

Educateagainsthate provides practical advice and support on protecting children from extremism and radicalisation

London Grid for Learning provides advice on all aspects of a school or college's online safety arrangements

NSPCC E-safety for schools provides advice, templates, and tools on all aspects of a school or college's online safety arrangements

Safer recruitment consortium "guidance for safe working practice", which may help ensure staff behaviour policies are robust and effective

Searching screening and confiscation is departmental advice for schools on searching children and confiscating items such as mobile phones

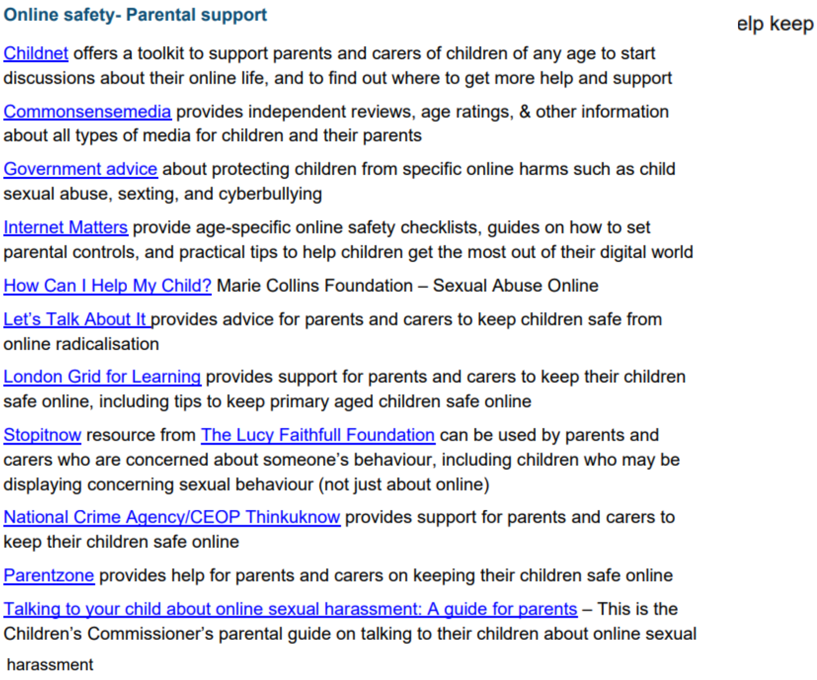
South West Grid for Learning provides advice on all aspects of a school or college's online safety arrangements

Use of social media for online radicalisation – A briefing note for schools on how social media is used to encourage travel to Syria and Iraq

Online Safety Audit Tool from UK Council for Internet Safety to help mentors of trainee teachers and newly qualified teachers induct mentees and provide ongoing support, development and monitoring

Online safety guidance if you own or manage an online platform – DCMS advice

A business guide for protecting children on your online platform – DCMS advice



## Online safety- Parental support

elp keep

Childnet offers a toolkit to support parents and carers of children of any age to start discussions about their online life, and to find out where to get more help and support

Commonsensemedia provides independent reviews, age ratings, & other information about all types of media for children and their parents

Government advice about protecting children from specific online harms such as child sexual abuse, sexting, and cyberbullying

Internet Matters provide age-specific online safety checklists, guides on how to set parental controls, and practical tips to help children get the most out of their digital world

How Can I Help My Child? Marie Collins Foundation – Sexual Abuse Online

Let's Talk About It provides advice for parents and carers to keep children safe from online radicalisation

London Grid for Learning provides support for parents and carers to keep their children safe online, including tips to keep primary aged children safe online

Stopitnow resource from The Lucy Faithfull Foundation can be used by parents and carers who are concerned about someone's behaviour, including children who may be displaying concerning sexual behaviour (not just about online)

National Crime Agency/CEOP Thinkuknow provides support for parents and carers to keep their children safe online

Parentzone provides help for parents and carers on keeping their children safe online

Talking to your child about online sexual harassment: A guide for parents – This is the Children's Commissioner's parental guide on talking to their children about online sexual harassment

**Legalisation**

At the Carlton Junior Academy, we are aware of the legislative framework under which this Online Safety Policy and guidance has been produced. It is important to note that in general terms an action that is illegal if committed offline is also illegal if committed online. It is recommended that legal advice is sought in the advent of an online safety issue or situation. The Data Acceptable Use Policy also contains a list  of the relevant legislation and guidance.

**Computer Misuse Act 1990**

This Act makes it an offence to

- erase or amend data or programs without authority.
- obtain unauthorised access to a computer.
- "eavesdrop" on a computer.
- make unauthorised use of computer time or facilities.
- maliciously corrupt or erase data or programs.
- deny access to authorised users.

**Data Protection Act 1998**

This protects the rights and privacy of individual's data. To comply with the law, information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully. The Act states that person data must be

- fairly and lawfully processed.
- processed for limited purposes.
- adequate, relevant and not excessive.
- accurate.
- not kept longer than necessary.
- processed in accordance with the data subject's rights.
- secure.
- not transferred to other countries without adequate protection.

**General Data Protection Regulation (GDPR) May 25, 2018**

The GDPR has applied to organisations across the world since 25 May 2018. With the UK now set to leave the European Union, the UK has formalised GDPR into new legislation under the Data Protection Act 2018. GDPR will now sit alongside DPA, however, in most cases, the DPA will be referred to as a matter of law. GDPR was designed to modernise laws that protect the personal information of individuals.

Before GDPR started to be enforced, the previous data protection rules across Europe were first created during the 1990s and had struggled to keep pace with rapid technological changes. GDPR alters how businesses and public sector organisations can handle the information of their customers. It also boosts the rights of individuals and gives them more control over their information.

**Freedom of Information Act 2000**

The Freedom of Information Act gives individuals the right to request information held by public authorities. All public authorities and companies wholly owned by public authorities have obligations under the Freedom of Information Act. When responding to requests, they have to follow a number of set procedures.

**Communications Act 2003**

Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

**Malicious Communications Act 1988**

It is an offence to send an indecent, offensive, or threatening letter, electronic communication or other article to another person.

**Regulation of Investigatory Powers Act 2000**

It is an offence for any person to intentionally and without lawful authority intercept any communication. Monitoring or keeping a record of any form of electronic communications is permitted, in order to

- establish the facts.
- ascertain compliance with regulatory or self-regulatory practices or procedures.
- demonstrate standards, which are or ought to be achieved by persons using the system.
- investigate or detect unauthorised use of the communications system.
- prevent or detect crime or in the interests of national security.

- ensure the effective operation of the system.

Monitoring but not recording is also permissible, in order to

- ascertain whether the communication is business or personal.
- protect or support help line staff.

The academy reserves the right to monitor its systems and communications in line with its rights under this act.

**Trade Marks Act 1994**

This provides protection for Registered Trade Marks, which can be any symbol (words, shapes or digital/video images) that are associated with a particular set of goods or services. Registered Trade Marks must not be used without permission. This can also arise from using a Mark that is confusingly similar to an existing Mark.

**Copyright, Designs and Patents Act 1988**

It is an offence to copy all, or a substantial part of a copyright work. There are, however, certain limited user permissions, such as fair dealing, which means under certain circumstances permission is not needed to copy small amounts for non-commercial research or private study. The Act also provides for moral rights, whereby authors can sue if their name is not included in a work they wrote, or if the work has been amended in such a way as to impugn their reputation. Copyright covers materials in print and electronic form, words, digital/video images, sounds, TV broadcasts and other media (e.g. YouTube).

**Telecommunications Act 1984**

It is an offence to send a message or other matter that is grossly offensive or of an indecent, obscene or menacing character. It is also an offence to send a message that is intended to cause annoyance, inconvenience or needless anxiety to another that the sender knows to be false.

**Criminal Justice & Public Order Act 1994**

This defines a criminal offence of intentional harassment, which covers all forms of harassment, including sexual. A person is guilty of an offence if, with intent to cause a person harassment, alarm or distress, they

- use threatening, abusive or insulting words or behaviour, or disorderly behaviour; or
- display any writing, sign or other visible representation, which is threatening, abusive or insulting, thereby causing that or another person harassment, alarm or distress.

**Racial and Religious Hatred Act 2006**

This Act makes it a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

**Protection from Harassment Act 1997**

A person must not pursue a course of conduct, which amounts to harassment of another, and which he/she knows or ought to know amounts to harassment of the other. A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him/her is guilty of an offence.

**Protection of Children Act 1978**

It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent digital/video images of children in the United Kingdom. A child for these purposes is anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital/video image. A digital/video image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison.

**Sexual Offences Act 2003**

A grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet). It is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. (Typically, teachers, social workers, health professionals, connexions staff fall in this category of trust). Any sexual intercourse with a child under the age of 13 commits the offence of rape.

**Public Order Act 1986**

This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence. Children, Families and Education Directorate page 38 April 2007.

**Obscene Publications Act 1959 and 1964**

Publishing an “obscene” article is a criminal offence. Publishing includes electronic transmission.

**Human Rights Act 1998**

This does not deal with any particular issue specifically or any discrete subject area within the law. It is a type of "higher law", affecting all other laws. In the academy context, human rights to be aware of include

- the right to a fair trial.
- the right to respect for private and family life, home and correspondence.
- freedom of thought, conscience and religion.
- freedom of expression.
- freedom of assembly.
- prohibition of discrimination.
- the right to education.

These rights are not absolute. The academy is obliged to respect these rights and freedoms, balancing them against those rights, duties and obligations, which arise from other relevant legislation.

**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.

**The Education and Inspections Act 2011**

Extended the powers included in the 2006 Act and gave permission for Headteachers (and nominated staff) to search for electronic devices. It also provides powers to search for data on those devices and to delete data.
http://www.education.gov.uk/academys/pupilsupport/behaviour/behaviourpolicies/f0076897/screening-searching-and-confiscation)

**The Protection of Freedoms Act 2012**

Requires academys to seek permission from a parent/carer to use Biometric systems.

**The Academy Information Regulations 2012**

Requires academys to publish certain information on its website:
https://www.gov.uk/guidance/what-maintained-academys-must-publish-online

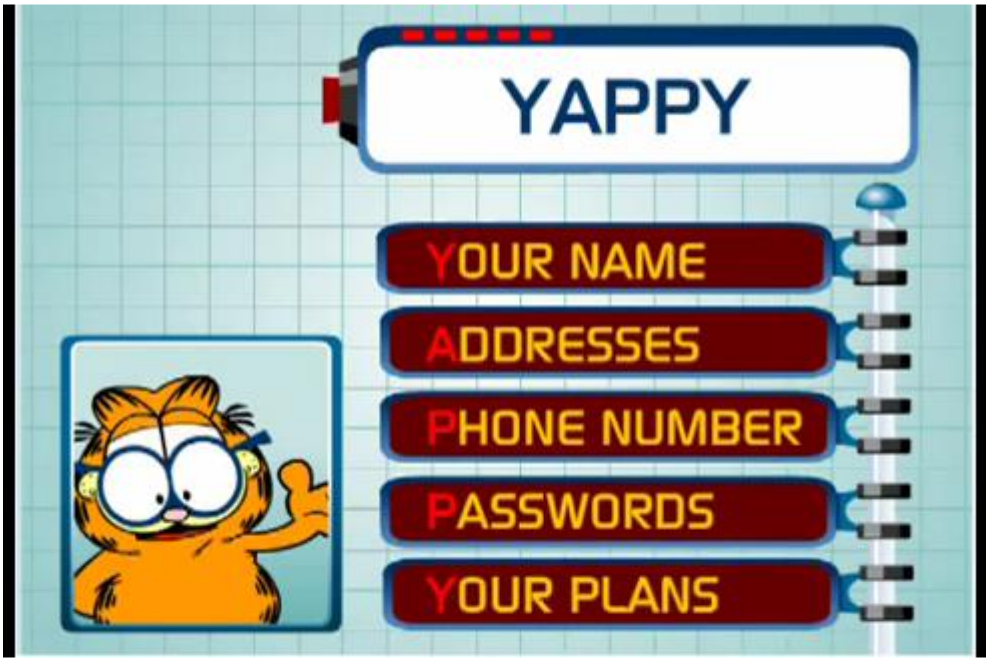
**Serious Crime Act 2015**

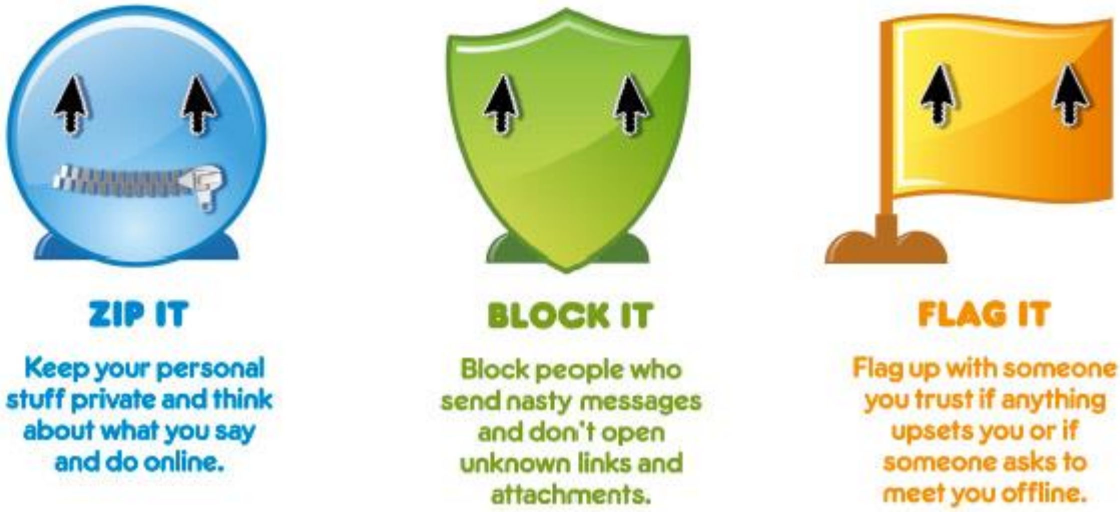
Introduced new offence of sexual communication with a child. Also created new offences and orders around gang crime (including CSE).

**Criminal Justice and Courts Act 2015**

Revenge porn – as it is commonly known - involves the distribution of private and personal explicit images or video footage of an individual or group without their consent, with the intention of causing them embarrassment and distress. Often revenge porn is used maliciously to shame partners. Revenge porn was made an offense in the Criminal Justice and Courts Act 2015. The Act specifies that if you are accused of revenge porn and found guilty of the criminal offence, you could be prosecute and face a sentence up to two years in prison.

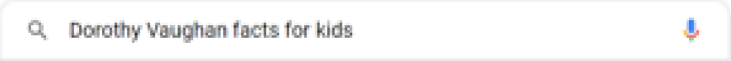
**Posters to be displayed in the academy**




ZIP IT
Keep your personal stuff private and think about what you say and do online.
BLOCK IT
Block people who send nasty messages and don't open unknown links and attachments.
FLAG IT
Flag up with someone you trust if anything upsets you or if someone asks to meet you offline.

# Our Academy's World Wide Web Online Safety Rules

1. When searching on the World Wide Web always type facts for kids after the thing you are searching for.

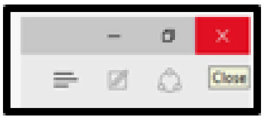


Dorothy Vaughan facts for kids

2. If you see something on the World Wide Web when you are using a laptop, that makes you feel uncomfortable, close the lid immediately and then tell the adult in the room.

3. If you see something on the World Wide Web when you are using an iPad that makes you feel uncomfortable, turn it over, put it on the desk and then tell the adult in the room.

4. Never get rid of or close the webpage as we need to report it to our technician so that they can stop anyone else from seeing it.



5. When you are connected to the internet, you must always be supervised by a member of staff.

**Glossary of Terms**

| | |
|---|---|
| **AUP/AUA** | Acceptable Use Policy / Agreement – |
| **CEOP** | Child Exploitation and Online Protection Centre (part of UK Police, dedicated to protecting children from sexual abuse, providers of the Think U Know programmes. |
| **CPD** | Continuous Professional Development |
| **FOSI** | Family Online Safety Institute |
| **ICO** | Information Commissioners Office |
| **ICT** | Information and Communications Technology |
| **ICTMark** | Quality standard for academys provided by NAACE |
| **INSET** | In Service Education and Training |
| **IP address** | The label that identifies each computer to other computers using the IP (internet protocol) |
| **ISP** | Internet Service Provider |
| **ISPA** | Internet Service Providers' Association |
| **IWF** | Internet Watch Foundation |
| **LA** | Local Authority |
| **LAN** | Local Area Network |
| **LSCB** | Local Safeguarding Children Board |
| **MIS** | Management Information System |
| **NEN** | National Education Network – works with the Regional Broadband Consortia (e.g. SWGfL) to provide the safe broadband provision to academys across Britain. |
| **Ofcom** | Office of Communications (Independent communications sector regulator) |
| **SWGfL** | South West Grid for Learning Trust – the Regional Broadband Consortium of SW Local Authorities – is the provider of broadband and other services for academies and other organisations in the SW |
| **TUK** | Think U Know – educational online safety programmes for academys, young people and parents. |
| **VLE** | Virtual Learning Environment (a software system designed to support teaching and learning in an educational setting, |
| **WAP** | Wireless Application Protocol |
| **UKSIC** | UK Safer Internet Centre – EU funded centre. Main partners are SWGfL, Childnet and Internet Watch Foundation. |

Note – this policy should be read in conjunction with our 'Permissions' forms, which are sent out to parents at the start of each academic year. These contain guidance/restrictions around photographic/film consent, codes of conduct (parent and child) and other similar agreements.