Robert Mellors Primary Academy

Online Safety Policy

Approving Body	Headteacher
Date Approved	TBC – Autumn term LAB meeting
Version	Version 1.0 July 2021
Supersedes Version	-
Review Date	Summer 2022
Further Information/Guidance	Keeping Children Safe in Education (2021)

Introduction

At Robert Mellors Primary Academy we are committed to ensuring that children learn how to use computers, ICT and modern technologies safely so that they:

- Are able to use ICT safely to support their learning in school
- Know how to use a range of ICT equipment safely
- Are able to use ICT and modern technologies outside school in a safe manner, including using ICT as a tool for communication
- Are prepared for the constant changes in the world of technology and understand how to use new and emerging technologies in a safe manner
- Know what to do if they feel unsafe when it comes to using technology and ICT

This policy outlines the steps the school takes to protect children from harm when using ICT and also how the school proactively encourages children to develop a safe approach to using ICT whether in school or at home.

The Law

Our Online Safety Policy has been written by the school, using advice from Nottingham County Council and government guidance. The Policy is part of the school's Strategic Development Plan and related to other policies including Positive Learning, Safeguarding and Data Protection policies.

As legislation is often amended and new regulations introduced the references made in this policy may be superseded. For an up to date list of legislation applying to schools please refer to the Department for Education website at www.education.gov.uk/schools.

Policy Development

The Online Safety Policy is part of the School Development Plan and relates to other policies including those for ICT, Anti-bullying and safeguarding children. Teaching of online safety will complement the Relationships Education curriculum, covering the principles of online safety at all key stages, with progression in the content to reflect the different and escalating risks that pupils face. This includes how to use technology safely, responsibly, respectfully and securely, and where to go for help and support when they have concerns about content or contact on the internet or other online technologies.

- Our policy has been written with full consultation from staff in school, parents/carers, governors and young people.
- It has been agreed by senior managers and approved by governors
- The policy and its implementation will be reviewed annually.
- It is available to read or download on our school website or you could request a hard copy from the school office.

Roles and Responsibilities

The Headteacher, alongside the Online Safety Co-ordinator (Andrew Emsley) will:

- Ensure the policy is implemented, communicated and compliance with the policy is monitored
- Ensure staff training in Online Safety is provided and updated annually as part of safeguarding training
- Ensure immediate action is always taken if any risks or dangers are identified i.e. reporting of inappropriate websites
- Ensure that all reported incidents of cyber bullying are investigated
- Ensure appropriate web filtering software is used to protect users from potentially damaging/offensive material

Teachers and Staff will ensure:

- they have an up-to-date awareness of online safety matters and of the current academy Online Safety Policy and practices.
- they have read ‘Keeping Children Safe in Education’ and understand the advice for schools on embedding online safety into their broader safeguarding and child protection approach. See appendix for Annex C of ‘Keeping Children Safe in Education’.
- they have read, understood and signed the Staff Acceptable Use Policy (AUP).
- they report any suspected misuse or problem to the Headteacher/Senior Leader/Online Safety Lead for investigation/action/sanction.

- all digital communications with pupils/parents/carers should be on a professional level and are only carried out using official academy systems.
- online safety issues are embedded in all aspects of the curriculum and other activities.
- pupils understand and follow the Online Safety Policy and Acceptable Use Policies.
- pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- they monitor the use of digital technologies, mobile devices, cameras etc in lessons and other academy activities (where allowed) and follow the academy's procedures with regard to these devices.
- they act as good role models in their use of digital technologies, the internet and mobile devices.
- in lessons where internet use is pre-planned, that they guide pupils to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- where pupils are allowed to freely search the internet, they should be vigilant in monitoring the content of the websites the young people visit.
- That 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 Technical Staff (or other relevant designated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

To support the delivery of an E-safe curriculum staff will refer to:

- Teaching Online Safety in School; DfE 2019
- Education for a Connected World framework; UK Council for Internet Safety 2018

Governors will:

- Ensure that the school is implementing this policy effectively
- Adhere to the acceptable use agreement when in school
- Have due regard for the importance of Online Safety in school

Network Manager/Technical staff will ensure that:

- the academy's technical infrastructure is as secure as possible and is not open to misuse or malicious attack.
- the academy meets required online safety technical requirements.
- staff users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed.
- the filtering is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person.
- any misuse of the network/internet/RMUnify/email is reported to the Headteacher or the Online Safety Lead.

- RM Broadband monitors internet activity.

Pupils are responsible for:

- using the academy digital technology systems in accordance with the Pupil Acceptable Use Agreement.
- having a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- understanding the importance of reporting abuse, misuse or access to inappropriate materials and knowing how to do so.
- knowing and understanding policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking/use of images and on online-bullying.
- understanding the importance of adopting good online safety practice when using digital technologies out of the academy and realising that the academy's Online Safety Policy covers their actions out of the academy, if related to their membership of the academy.

Parents and carers

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

- digital and video digital/video images taken at academy events.
- the parents' sections of the website and on-line programmes the academy uses.
- their children's personal devices in the academy (where this is allowed).
- social media.

Community Users

Community Users who access academy systems/website and other online programmes as part of the wider academy provision will be expected to sign a Community User AUA before being provided with access to academy systems.

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.

Teaching and Learning

Why internet and digital communications are important.

- The purpose of any technology in school is to raise educational standards, to promote achievement, to support the professional work of staff and to enhance the school's management functions.
- Our school has a duty to provide students with a quality internet access as part of their learning experience.
- Internet use is part of the statutory curriculum and a necessary tool for staff.
- Pupils will be educated in the safe, effective use of the internet, including the skills of knowledge location, retrieval and evaluation.
- They will be encouraged to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- pupils will be shown how to publish and present information appropriately to a wider audience.
- They will be taught what internet use is acceptable and what is not and given clear objectives for use. These are also important transferable skills for their life out of school, including using mobile phones and other mobile devices.
- They will be taught how to report unpleasant internet content including cyberbullying or unwanted contact. This will include using the CEOP icon.
- Issues such as Cyberbullying and Online Safety will be built into the curriculum to encourage self-efficacy and resilience. Some children who have had problems or with additional needs may need additional support.

The school will actively teach Online Safety at an age-appropriate level. The school follows government guidance (including Education for a Connected World framework) allowing coverage of: what should and shouldn't be shared online, password control and cyber bullying among other topics. Online Safety will also be embedded throughout learning whenever children are using ICT in other lessons following the Knowsley City Learning Centres Scheme of work to ensure all content is up to date and appropriate

Pupils should:

- STOP and THINK before they CLICK.
- use YAPPY and ZIP IT, BLOCK IT, FLAG IT to stay safe online.
- Pupils should be taught that being online can put them at risk of sexual abuse, emotional abuse and Child-on-Child/Peer-on-Peer abuse.
- understand why and how some people will 'groom' young people for sexual or radicalisation reasons.
- be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making. (The Counter Terrorism and Securities Act 2015 which requires academies to ensure that children are safe from terrorist and extremist material on the internet).
- understand the impact of online bullying, sexting, extremism and trolling and know how to seek help if they are affected by any form of online bullying.
- be aware that anyone can watch live streaming and can share live streams through other Apps if the privacy settings on each App is not switched on.
- understand how video/digital images can be manipulated and how web content can attract the wrong sort of attention.
- understand why online 'friends' may not be who they say they are and to understand why they should be careful in online environments.
- understand why they should not post or share detailed accounts of their personal lives, contact information, daily routines, location, photographs and videos and to know how to ensure they have turned-on privacy settings.
- understand why they must not post pictures or videos of others without their permission.
- know not to download any files – such as music files - without permission.
- have strategies for dealing with receipt of inappropriate materials.
- know how to report any abuse including online bullying; and how to seek help if they experience problems when using the internet and related technologies, i.e. Parent/Carer, teacher or trusted staff member, or an organisation such as ChildLine or the CLICK CEOP button.
- be taught in all lessons to be critically aware of the materials/content they access online and be guided to validate the accuracy of information.
- be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- be aware that the author of a website/page may have a particular bias or purpose and to develop skills to recognise what that may be.

- know how to narrow down or refine a search understanding how search engines work and that this affects the results they see at the top of the listings.
- understand the issues around aspects of the commercial use of the internet, as age appropriate. This may include risks in pop-ups, buying online and online gaming or gambling.
- be helped to understand the need for the Pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside of the academy.

Parents/Carers

Many parents and carers have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring/regulation of the children's online behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.
The academy will therefore seek to provide information and awareness to parents and carers through:

- Curriculum activities.
- Letters, newsletters, website.
- Parents'/Carers' evenings and sessions.
- High profile events/campaigns e.g. Safer Internet Day.
- Sending home the Digital Parenting Magazine and other information sheets.
- Reference to the relevant websites/publications on the academy website (see appendix for further links/resources).
- The Wider Community
- The academy will provide opportunities for local community groups/members of the community to gain from the academy's online safety knowledge and experience. This may be offered through the following:
- Providing family learning courses in use of new digital technologies, digital literacy and online safety.
- Targeting Online Safety messages towards grandparents and other relatives as well as parents.
- Providing online safety information for the wider community via the academy website.

Staff/Volunteers

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

- A planned programme of formal online safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out regularly.

- All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the academy’s Safeguarding procedures, Online Safety Policy and Acceptable Use Agreements.
- The Online Safety Lead will receive regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisations.
- This Online Safety Policy and its updates will be presented to and discussed by staff in staff meetings.
- The Online Safety Lead will provide advice/guidance/training to individuals as required.

Governors

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

- Attending training provided by the Local Authority/MAT/National Governors association/or other relevant organisation if available.
- Participating in academy training/information sessions for staff or parents. This may include attending assemblies or lessons.

Monitoring safe and secure systems

Internet access is regulated by RM Unify filtered broadband connection which blocks access to unsuitable websites in accordance with the UK Safer Internet Centre guidance. Antivirus software has been installed on all computers and is to be maintained and updated regularly. Staff passwords are changed regularly and must be strong passwords. Staff take responsibility for safeguarding confidential data saved to laptops, i.e. use of strong passwords. If personal data has to be saved to other media, e.g. data sticks or CDs, it is to be encrypted or strong password protected, staff have been trained to use OneDrive to ensure data remain secure and password protected at all times. Staff with access to the ICT systems containing confidential and personal data are to ensure that such data is properly protected at all times.

Safe use of the Internet and Web Filtering

- All staff and pupils will have access to the internet through the school’s network
- All staff, volunteers who have use of the school’s IT equipment, must read and sign the Staff Acceptable Use Agreement.
- All children must read and sign the Pupil Acceptable Use Agreement.
- If a site containing inappropriate material is encountered, children must report it to an adult who will report it to the Headteacher or Online Safety Coordinator to pass to Schools IT, the IT services provider
- If an adult finds a site that they consider unsuitable they should report it to the Headteacher or Online Safety Coordinator

The use of Email

All teaching and support staff are provided with a school email address. Staff should use this address when sending work-related emails All emails should be professional in nature and staff should be aware that all emails can be retrieved at a later date should this be necessary. Staff emails should never be used to forward 'chain' or 'junk' email. Staff should not communicate with pupils via email.

The school website

- The school web site complies with statutory DFE requirements
- Images that include pupils will be selected carefully and only used if parents have given permission for such images to be posted on line.

Social Networking, Social Media and Personal Publishing (blogging)

The school recognises that it has a duty to help keep children safe when they are accessing such sites at home, and to this end the school will cover such issues within the curriculum. Pupils will not access social networking sites, e.g. Facebook or Twitter in school. They will be taught about how to stay safe when using such sites at home.

Staff private use of social media:

- No reference should be made in social media to students / pupils, parents /carers / school staff or issues / situations related to the school
- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to the school
- Security settings on personal social media profiles should be regularly checked to minimise risk of loss of personal information.
- Teachers are instructed not to run social network spaces for student use on a personal basis or to open up their own spaces to their students, but to use the schools' preferred system for such communications.
- Staff are not permitted to maintain a Social Media relationship with any pupil, current or alumni until such time that the pupil turns 18.

The Use of Cameras, Video and Audio Recording Equipment

Staff may only use the school's photographic or video devices to support school trips and curriculum activities. Photos should only be uploaded to the school system. They should never upload images to the internet unless specific arrangements have been agreed with the Headteacher or Deputy Headteacher, nor circulate them in electronic form outside the school. It is never acceptable to use photographic or video devices in changing rooms or toilets

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 or carers will be obtained before any digital/video images of pupils are published on the academy website, SeeSaw, 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.
- 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.
- In accordance with guidance from the Information Commissioner's Office, parents/ carers are welcome to take videos and digital images of their children at academy events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases child protection, these digital/video images should not be published/made publicly available on social networking sites, nor should parents/carers comment on any activities involving other pupils in the digital/video images.
- 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.
- 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 and the children will be taught about the need to keep these digital/video images private. When on academy visits, pupils are not allowed to take their own cameras or use cameras on phones without permission.
- 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.
- Pupils must not take, use, share, publish or distribute digital/video images of others without their permission.
- 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
- 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 school 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.
- 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.

Personal mobile phones and mobile devices

- Use of mobiles is discouraged throughout the school, particularly in certain areas. The areas which should be considered most vulnerable include: toilets and changing areas, including where children change for swimming.
- The school reserves the right to search the content of any mobile or handheld devices on the school premises where there is a reasonable suspicion that it may contain undesirable material, including those which promote pornography, violence or bullying. Staff mobiles or hand-held devices may be searched at any time as part of routine monitoring at the direction of the Headteacher.
- Staff are only permitted to use their own mobile phones or devices for contacting children, young people or their families within or outside of the setting in a professional capacity at the Headteachers discretion (e.g. for emergency contact relating to the safety or wellbeing of a child whilst on an educational visit).

Data Protection

- With effect from 25th May 2018, the data protection arrangements for the UK changed following the European Union General Data Protection Regulation (GDPR). As a result, academies are likely to be subject to greater scrutiny in their care and use of personal data.
- Personal data will be recorded, processed, transferred and made available according to the current data protection legislation.
- The academy has ensured that it has a GDPR Policy, Pupil and Staff Privacy Notices and a Trust Data Acceptable use Statement.

Communications

- When using communication technologies the academy considers the following as good practice.
- The official academy email service may be regarded as safe and secure and is monitored.
- Users should be aware that email communications can be monitored.
- Users must immediately report, to the nominated persons – in accordance with the academy policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Any digital communication between staff and pupils or parents/carers (email, social media, chat, blogs, etc.) must be professional in tone and content. These communications may only take place on official academy systems. Personal email

addresses, text messaging or social media must not be used for these communications.

- Pupils may be provided with individual academy email addresses for educational use.
- Pupils should be taught about online safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
- Users should know that spam, phishing and virus attachments can make emails dangerous.
- Users should know that email sent to an external organisation must be written carefully, (and may require authorisation), in the same way as a letter written on academy headed paper.
- Users should know that the sending of multiple or large attachments should be limited, and may also be restricted by the provider of the service being used.
- Personal information should not be posted on the academy website.
- The academy does not publish personal email addresses of pupils or staff on the academy website. There is a link to staff email so that children can hand in homework but the staff email address cannot be seen by users of the website.
- Social Media - Protecting Professional Identity
- Our academy has a duty of care to provide a safe learning environment for pupils and staff. The academy could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, engage in online bullying, discriminate on the grounds of sex, race or disability or who defame a third party may render the academy liable to the injured party. Reasonable steps to prevent predictable harm must be in place. The academy provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the academy through:
    - ensuring that personal information is not published.
    - ensuring training is provided including: acceptable use; social media risks; checking of settings; data protection and reporting issues.
    - clear reporting guidance, including responsibilities, procedures and sanctions.
    - risk assessment, including legal risk.

Academy staff should ensure that:

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

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

- a process for approval by senior leaders.
- a clear process for the administration and monitoring of these accounts – involving at least two members of staff.
- a code of behaviour for users of the accounts.
- systems for reporting and dealing with abuse and misuse.
- an understanding of how incidents may be dealt with under academy disciplinary procedures.

Personal Use

- Personal communications are those made via personal social media accounts. In all cases, where a personal account is used which associates itself with the academy or impacts on the academy, it must be made clear that the member of staff is not communicating on behalf of the academy with an appropriate disclaimer. Such personal communications are within the scope of this policy.
- Personal communications which do not refer to or impact upon the academy are outside the scope of this policy.
- The academy permits reasonable and appropriate access to private social media sites.
- Where excessive personal use of social media in the academy is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken.

Monitoring of Public Social Media

- As part of active social media engagement, it is considered good practice to pro-actively monitor the Internet for public postings about the academy.
- The academy should effectively respond to social media comments made by others according to a defined policy or process.
- The academy's use of social media for professional purposes will be checked regularly by the Senior Leadership Team to ensure compliance with the academy policies.

Academy Website

- The Headteacher takes overall responsibility to ensure that the website content is accurate and the quality of presentation is maintained.
- 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.
- 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.

- 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.

SeeSaw

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 school 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.
- Staff use the same professional language and tone as 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, school dinners or complaints should go to the school 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 SeeSaw 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 SeeSaw.
- Parents/Carers will not use the site in any way that is harmful to minors. Pupils
- Pupils should not be using SeeSaw to communicate with their class teacher.

Cloud-Based Technologies

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

YouTube Videos

- Videos can only be uploaded to the academy YouTube channel by the designated member of staff, 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.

Watching 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 school filters deny access to YouTube on pupil logins.

Live Streaming/Video Conferencing on Site

- Facebook Live, Zoom, Instagram Live and YouTube Live are not used to live stream in the academy. Skype/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, Zoom, Instagram Live and YouTube Live are not used to live stream in the academy. Microsoft Teams 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 school 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.

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.

Staff WhatsApp Groups

- Never grant pupils access to your device.
- Always use the same professional language and tone as you would in person.
- Always think carefully before sharing information, pictures or videos and make sure they are appropriate and linked to work matters.
- Check your privacy settings (e.g. profile pic to be seen, “last seen” status, ‘read’ receipts disabled etc)
- Ensure adherence to good practice on naming of children (i.e. initials only).
- Do not share personal information.
- Do not post content at unreasonable times of day.

Management of online safety incidents

There is strict monitoring and application of the Online Safety policy and a differentiated and appropriate range of sanctions; all members of the school are encouraged to be vigilant in reporting issues, in the confidence that issues will be dealt with quickly and sensitively, through the school’s escalation processes;

- Support is actively sought from other agencies as needed (i.e. MASH, UK Safer Internet Centre helpline, CEOP, Prevent Officer, Police, IWF) in dealing with online safety issues;
- Monitoring and reporting of online safety incidents takes place and contribute to developments in policy and practice in online safety within the school;
- Parents/carers are specifically informed of online safety incidents involving young people for whom they are responsible;
- The Police will be contacted if one of our staff or pupils receives online communication that we consider is particularly disturbing or breaks the law;
- We will immediately refer any suspected illegal material to the appropriate authorities – Police, Internet Watch Foundation and inform MASH.

Dealing with unsuitable / inappropriate activities

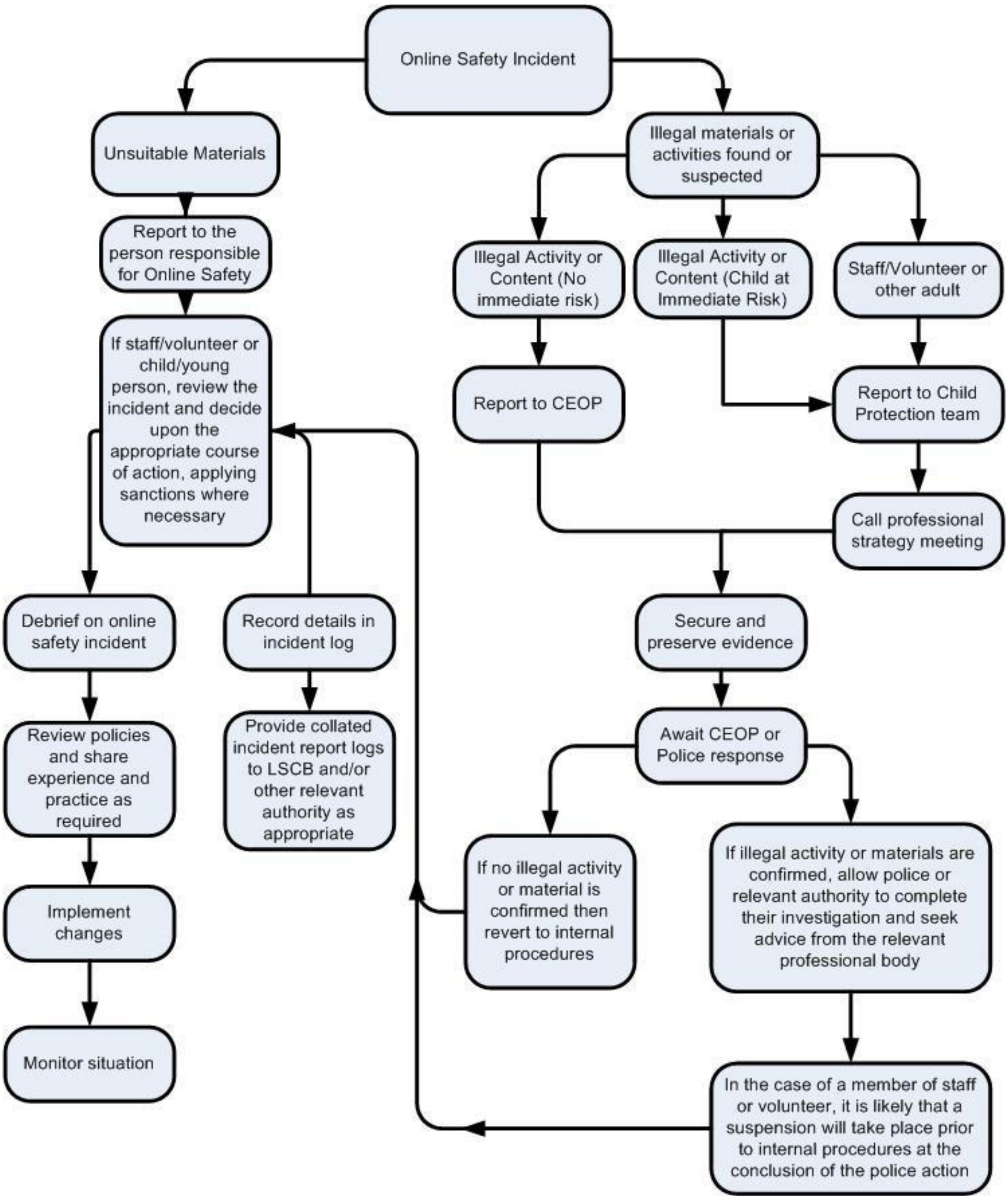
Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned from the academy and all other technical systems. Other activities e.g. cyber-bullying would be banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would be inappropriate in an academy context, either because of the age of the users or the nature of those activities.

User Actions		Acceptable at certain times	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to the Protection of Children Act 1978			X
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.			X
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character). Contrary to the Criminal Justice and Immigration Act 2008			X
	Criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation). Contrary to the Public Order Act 1986			X
	Maliciously corrupt or erase data or programs. Contrary to the Computer Misuse Act 1990.			X
	Promotion of any kind of discrimination. Contrary to the Racial and Religious Hatred Act 2006 and the Public Order Act 1986.			X
	Threatening behaviour, including promotion of physical violence or mental harm. Contrary to the Malicious Communications Act 1988.			X
	Promotion of extremism or terrorism. Contrary to the Racial and Religious Hatred Act 2006.			X
	Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the academy or brings the academy			X
	into disrepute. .Contrary to the Communications Act 2003.			

	Using academy systems to run a private business. Contrary to the Computer Misuse Act 1990. .			X
	Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the academy. Contrary to the Regualtion of Investigatory Powers Act 2000.			X
	Infringing copyright. Contrary to the Copyright, Design and Patents Act 1988.			X
	Revealing or publicising confidential or proprietary information (eg financial/personal information, databases, computer/network access codes and passwords). Contrary to the Computer Misuse Act 1990.			X
	Creating or propagating computer viruses or other harmful files. Contrary to the Computer Misuse Act 1990.			X
Unfair usage (downloading/uploading large files that hinders others in their use of the internet)			X	
On-line gaming (educational)		X		
On-line gaming (non-educational)			X	
On-line gambling			X	
On-line shopping / commerce		X		
File sharing		X		
Use of social media		X		
Use of messaging apps		X		
Use of video broadcasting e.g. YouTube		X		

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 academy 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 Headt eacher /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 sancti on 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 Headt eacher /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

Working in Partnership with Parents

Parents' attention will be drawn to the Online Safety Policy through the school newsletters, information evenings and on the school website. A partnership approach with parents will be encouraged. Parents will be requested to sign an Acceptable Use Agreement as part of the Home School Agreement on entry to the school.

Protecting School Staff

In order to protect school staff we require that parents do not comment on school issues or staff using social networking sites. Any concerns or complaints should be discussed directly with the school. The school will take action if there is evidence that inappropriate comments about staff have been placed on the internet in a public arena.

Safeguarding – scope of this policy

(See also Safeguarding and behaviour policies)

The Education and Inspections Act 2006 empowers the Headteacher to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other Online Safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school.

The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the school's Behaviour Management Policy.

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

Internet Access Policies

The schools' Internet Access Policy is part of the ICT policy but will also link to other policies, including those for behaviour and PSHE.

The purpose of Internet access in school is to contribute to the quality of our curriculum provision, to raise attainment, to support the children's learning across the curriculum, to help with the workload of all staff and to enhance the schools' management and administrative systems.

Access to the Internet is a necessary tool for all staff and a curriculum entitlement for the children. The use of school equipment to access the Internet brings with it a responsibility for its use. The use of a computer system without permission or for a purpose not agreed by the school could constitute a criminal offence under the Computer Misuse Act 1990.

The benefits of Internet access in school

- Enjoying using the internet to find information across the curriculum.
- Learning how to use search engines to retrieve information.
- Access to educational resources through the world-wide-web, including libraries, museums and art galleries.
- Rapid and cost effective world-wide communication.
- Access to news and current events from the perspective of a range of people and cultures.
- Access to discussion with experts in many fields for pupils and staff via email.
- Staff professional development through access to educational materials and good curriculum practice.
- Communication between schools, with support services, other teachers and other professionals.
- Exchange of curriculum and administration data with the LEA and DfEE.
- Social and leisure use during supervised computer clubs.

Legislation

At Robert Mellors Primary 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.

- **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/schools/pupilsupport/behaviour/behaviourpolicies/f0076897/screenin g-searching-and-confiscation)

The Protection of Freedoms Act 2012

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

- **The School Information Regulations 2012**

Requires schools to publish certain information on its website: https://www.gov.uk/guidance/what-maintained-schools-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).

Links to other Organisations or Documents

UK Safer Internet Centre
Safer Internet Centre – https://www.saferinternet.org.uk/
South West Grid for Learning - https://swgfl.org.uk/products-services/online-safety/ Childnet – http://www.childnet-int.org/
Professionals Online Safety Helpline - http://www.saferinternet.org.uk/about/helpline
Internet Watch Foundation - https://www.iwf.org.uk/
LGfL – Online Safety Resources
Kent – Online Safety Resources page
INSAFE / Better Internet for Kids - https://www.betterinternetforkids.eu/
UK Council for Child Internet Safety (UKCCIS) - www.education.gov.uk/ukccis
Netsmartz - http://www.netsmartz.org/
CEOP - http://ceop.police.uk/
ThinkUKnow - https://www.thinkuknow.co.uk/

Tools for Schools
Online Safety BOOST – https://boost.swgfl.org.uk/
360 Degree Safe – Online Safety self-review tool – https://360safe.org.uk/
360Data – online data protection self review tool: www.360data.org.uk

Bullying/Online-bullying/Sexting/Sexual Harassment
Enable – European Anti Bullying programme and resources (UK coordination / participation through
SWGfL & Diana Awards) - http://enable.eun.org/
Scottish Anti-Bullying Service, Respect me - http://www.respectme.org.uk/ Scottish Government - Better relationships, better learning, better behaviour - http://www.scotland.gov.uk/Publications/2013/03/7388 DfE - Online bullying guidance - https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/374850/Online
bullying_Advice_for_Headteachers_and_School_Staff_121114.pdf Childnet – Online bullying guidance and practical PSHE toolkit: http://www.childnet.com/our-projects/online bullying -guidance-and-practical-toolkit
Childnet – Project deSHAME – Online Sexual Harassment

UKSIC – Sexting Resources
Anti-Bullying Network – http://www.antibullying.net/online bullying 1.htm
Ditch the Label – Online Bullying Charity
Diana Award – Anti-Bullying Campaign

Social Networking
Digizen – Social Networking
UKSIC - Safety Features on Social Networks
Children's Commissioner, TES and Schillings – Young peoples' rights on social media

Curriculum
SWGfL Digital Literacy & Citizenship curriculum
UKCCIS – Education for a connected world framework
Teach Today – www.teachtoday.eu/ Insafe - Education Resources

Mobile Devices/BYOD
Cloudlearn Report Effective practice for schools moving to end locking and blocking NEN - Guidance Note - BYOD

Data Protection
360data - free questionnaire and data protection self review tool

ICO Guide for Organisations (general information about Data Protection)

ICO Guides for Education (wide range of sector specific guides)
DfE advice on Cloud software services and the Data Protection Act

ICO Guidance on Bring Your Own Device

ICO Guidance on Cloud Computing

ICO - Guidance we gave to schools - September 2012

IRMS - Records Management Toolkit for Schools

NHS - Caldicott Principles (information that must be released)

ICO Guidance on taking photos in schools

Dotkumo - Best practice guide to using photos

Professional Standards/Staff Training
DfE – Keeping Children Safe in Education
DfE - Safer Working Practice for Adults who Work with Children and Young People
Childnet – School Pack for Online Safety Awareness
UK Safer Internet Centre Professionals Online Safety Helpline

Infrastructure/Technical Support
UKSIC – Appropriate Filtering and Monitoring
Somerset - Questions for Technical Support
NEN – Advice and Guidance Notes

Working with Parents and Carers
SWGfL Digital Literacy & Citizenship curriculum
Online Safety BOOST Presentations - parent's presentation
Vodafone Digital Parents Magazine
Childnet Webpages for Parents & Carers
Get Safe Online - resources for parents
Teach Today - resources for parents workshops / education
The Digital Universe of Your Children - animated videos for parents (Insafe)
Cerebra - Learning Disabilities, Autism and Internet Safety - a Parents' Guide Insafe - A guide for parents - education and the new media

Research
EU Kids on Line Report - "Risks and Safety on the Internet" - January 2011
Futurelab - "Digital participation - its not chalk and talk any more!"
Ofcom –Media Literacy Research

Redhill Academy Trust Safeguarding protocols during Coronavirus (Covid-19) and the enforced partial closure of schools.

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)