L.E.A.D. Academy Trust
Lead • Empower • Achieve • Drive

Rainbow Forge Primary Academy

Online Safety and Acceptable Use of Technology Policy

Agreed:

Review:

Content

	Page no
Policy Aims	5
Policy Scope	5
Policy Links	6
Monitoring and Review	
Part 1 – Pupils	7
1.1 Roles and Responsibilities	
1.2 Education and Engagement	7
1.3 Technical Security – Passwords	9
1.4 Filtering and Monitoring	9
1.5 Using and Publishing Images and Videos Online	10
1.6 Managing Email	10
1.7 Social Media	10
1.8 Mobile Technology – Use of Mobile Phones and Personal Devices	11
1.9 Concerns about Online Behaviour and/or Welfare	14
Part 2 – Staff/Adults	15
2.1 Roles and Responsibilities	15
2.2 Education and Engagement	17
2.3 Reducing Online Risks	17
2.4 Safer Use of Technology	18
2.5 Password Security	19
2.6 Filtering and Monitoring	20
2.7 Managing Safety of the Academy Website	20
2.8 Using and Publishing Images and Videos Online	21
2.9 School and Staff Email	21
2.10 Social Media	22
2.11 Streaming Media Sites	26
2.12Mobile Technology – Use of Mobile Phones and Personal Devices	28
2.13 Responding to Online Safety Incidents	29
2.14 Procedure for Responding to Specific Online Safety Incidents	39
2.15 Breaches	40
Responding to an Online Safety Concern Flowchart	
Part 3 – Academy/Trust	42
3.1 Roles and Responsibilities	42
3.2 Academy Technical Security – Passwords	42
3.3 Filtering and Monitoring	43
3.4 Managing Personal Data Online	45
3.5 Social Media	45
3.6 Electronic and Press Communication	

Part 4 – Parents/Carers 45
4.1 Roles and Responsibilities 46
4.2 Education and Engagement 46
4.3 Using and Publishing Images and Videos Online 46
4.4 Mobile Technology – Use of Mobile Phones and Personal Devices 46
4.5 Concerns about Parent/Carer Online Behaviour and/or Welfare 47

Part 5 – Visitors 47
5.1 Roles and Responsibilities 49
5.2 Mobile Technology – Use of Mobile Phones and Personal Devices 50--49

Appendices 50

Appendix 1 – Pupil Acceptable Use Agreement 50
Early Years and Key Stage 1 (0–6) 50
Key Stage 2 (7–11) 50
Key Stage 3/4/5 (11–18) 52
Pupils with SEND 54
Pupil Acceptable Use Agreement Form 56

Appendix 2 – Parent Acceptable Use Agreement 57
Parent/Carer Acknowledgement Form 58
Parent/Carer Acceptable Use Agreement 58

Appendix 3 – Staff Acceptable Use Agreement 59

Appendix 4 – Visitor Acceptable Use Agreement 66

Appendix 5 – Wi-Fi Acceptable Use Agreement 69

Appendix 6 – Remote Learning Guidance 71

Appendix 7 – Guidance on use of streaming media sites

Appendix 8 – Guidance for Parents on the use of Vimeo 78

Appendix 9 – Social Media Support Tools – examples and links 80

Key Details

Designated Safeguarding Lead (DSL): (Nina Sneddon, Deputy Headteacher)

Named governor with lead responsibility: (Andrew Blench)

Date written: (February 2023)

Date agreed and ratified by the governing body: (February 2023)

Date of next review: (February 2024)

This policy will be reviewed **at least** annually. It will also be revised following any concerns and/or updates to national and local guidance or procedures.

Rainbow Forge Academy Online Safety Policy

Policy Aims

This online safety policy has been written by Rainbow Forge Academy, involving staff, pupils and parents/carers. It takes into account the most recent DfE statutory guidance 'Keeping Children Safe in Education', Early Years and Foundation Stage 2017, 'Working Together to Safeguard Children' 2018 and the local Safeguarding Children Multi-agency Partnership procedures**.**

The purpose of Rainbow Forge Academy Online Safety policy is to:

- safeguard and promote the welfare of all members of Rainbow Forge community online
- identify approaches to educate and raise awareness of online safety throughout our community
- enable all staff to work safely and responsibly, to role model positive behaviour online and to manage professional standards and practice when using technology
- identify clear procedures to follow when responding to online safety concerns.

Rainbow Forge Academy understands that the issues associated with online safety are considerable but can be broadly categorised into three areas of risk:

1. **Content:** being exposed to illegal, inappropriate or harmful material.
2. **Contact:** being subjected to harmful online interaction with other pupils.
3. **Conduct:** personal (staff or pupils) online behaviour that increases the likelihood of, or causes, harm.
4. **Commerce**: risks such as online gambling, inappropriate advertising, phishing and or financial scams.

Policy Scope

Rainbow Forge Academy recognises that online safety is an essential part of safeguarding and acknowledges its duty to ensure that all pupils and staff are protected from potential harm online.

Rainbow Forge Academy identifies that the internet and associated devices, such as computers, tablets, mobile phones and games consoles are an important part of everyday life, which present positive and exciting opportunities, as well as challenges and risks.

Rainbow Forge Academy will empower our pupils to acquire the knowledge needed to use the internet and technology in a safe, considered and respectful way, and develop their resilience so they can manage and respond to online risks.

This policy applies to all staff, including the governing body, leadership team, teachers, support staff, external contractors, visitors, volunteers and other individuals who work for, or provide services on behalf of the setting (collectively referred to as 'staff' in this policy) as well as pupils and parents/carers.

This policy applies to all access to the internet and use of technology, including mobile technology, or where pupils, staff or other individuals have been provided with setting issued devices for use, both on and off site.

Links with other Policies and Practices

This policy links with several other policies, practices and action plans, including but not limited to:

- Anti-bullying policy
- Acceptable Use Agreements (AUA)
- Code of Conduct policy
- Staff Disciplinary policy
- Behaviour policy
- Safeguarding and Child Protection policy
- Confidentiality policy
- Curriculum policies, such as: Computing, Personal Social and Health Education (PSHE), and Relationships and Sex Education (RSE)
- Data Security policy
- Serious Violence and Weapons policy.

Monitoring and Review

Technology evolves and changes rapidly and, as such, Rainbow Forge Academy will review this policy at least annually. The policy will be revised following any national statutory guidance or local policy updates, any local child protection concerns and/or any changes to our technical infrastructure.

We will regularly monitor internet use and evaluate online safety mechanisms to ensure that this policy is consistently applied.

To ensure oversight of online safety, the Headteacher and L.E.A.D. IT will be informed of online safety concerns, as appropriate.

The named governor for safeguarding will report online safety practice and incidents, including outcomes, on a regular basis to the wider governing body.

Any issues identified via monitoring policy compliance will be incorporated into our action planning.

Part 1 – Pupils

1.1 Roles and Responsibilities

It is the responsibility of pupils (at a level that is appropriate to their individual age and ability) to:

- engage in age/ability-appropriate online safety education
- contribute to the development of online safety policies
- read and adhere to the Acceptable Use of Technology and Behaviour policies
- respect the feelings and rights of others, on and offline
- take an appropriate level of responsibility for keeping themselves and others safe online

- seek help from a trusted adult, if they are concerned about anything they or others experience online.

1.2 Education and Engagement

We will establish and embed a 'whole Academy' culture and will raise awareness and promote safe and responsible internet use amongst pupils by:

- ensuring our curriculum and whole Academy approach is developed in line with the UK Council for Internet Safety (UKCIS) 'Education for a Connected World Framework' and DfE 'Teaching online safety in school' guidance
- ensuring online safety is addressed in Relationships Education, RSE, PSHE and Computing programmes of study
- We use the Sheffield PSHE curriculum which has regular updates to ensure online resources are relevant.
- reinforcing online safety principles in other curriculum subjects as appropriate, and whenever technology or the internet is used on site
- creating a safe environment in which all pupils feel comfortable to say what they feel, without fear of getting into trouble and/or being judged for talking about something which happened to them online
- involving the DSL, as appropriate, as part of planning for online safety lessons or activities, so they can advise on any known safeguarding cases, and ensure support is in place for any pupils who may be impacted by the content
- making informed decisions to ensure that any educational resources used are appropriate for our pupils
- using external visitors, where appropriate, to complement and support our internal online safety education approaches
- providing online safety education as part of the transition programme across the key stages and/or when moving between establishments
- rewarding positive use of technology.

Rainbow Forge Academy will support pupils to understand and follow our AUAs in a way which suits their age and ability by:

- displaying acceptable use posters
- informing pupils that network and internet use will be monitored for safety and security purposes, and in accordance with legislation
- seeking learner voice when writing and developing online safety policies and practices, including curriculum development and implementation.

Rainbow Forge Academy will ensure pupils develop the underpinning knowledge and behaviours needed to navigate the online world safely, in a way which suits their age and ability by:

- ensuring age-appropriate education regarding safe and responsible use precedes internet access
- teaching pupils to evaluate what they see online and recognise techniques used for persuasion, so they can make effective judgements about if what they see is true, valid or acceptable

- educating them in the effective use of the internet to research, including the skills of knowledge location, retrieval and evaluation
- enabling them to understand what acceptable and unacceptable online behaviour looks like
- preparing them to identify possible online risks and make informed decisions about how to act and respond
- ensuring they know how and when to seek support if they are concerned or upset by something they see or experience online.

Vulnerable Pupils

Rainbow Forge Academy recognises that any learner can be vulnerable online, and vulnerability can fluctuate depending on their age, developmental stage, and personal circumstances. However, there are some pupils, for example Looked After Children and those with special educational needs, who may be more susceptible or may have less support in staying safe online.

Rainbow Forge Academy will ensure that differentiated and appropriate online safety education, access and support is provided to vulnerable pupils.

Staff at Rainbow Forge Academy will seek input from specialist staff as appropriate, including the DSL, SENCO, and Child in Care Designated Teacher to ensure that the policy and curriculum is appropriate to our community's needs.

1.3 Technical Security – Passwords

A safe and secure username/password system is essential if the above is to be established, and this applies to all Academy technical systems, including networks and devices.

Pupil passwords

All pupils in Rainbow Forge Academy will have clearly defined access rights to Academy technical systems and devices. Details of the access rights available to groups of pupils will be recorded by the Network Manager and will be reviewed, at least annually, by SLT/L.E.A.D. IT.

All Academy networks and systems will be protected by secure passwords that are regularly changed.

The 'master/administrator' passwords for the Academy systems, used by the technical staff, must also be available to the Headteacher or other nominated senior leader and kept in a secure place, e.g. the Academy safe. Consideration should also be given to using two-factor authentications for such accounts.

Passwords for new pupils, and replacement passwords for existing pupils, will be allocated by the Network Manager L.E.A.D. IT. Pupils will be required to change their password every term and will be taught the importance of password security.

All pupils (adults and young people) will have responsibility for the security of their username and password, and must not allow other adults or pupils to access the systems using their log-on details and must immediately report any suspicion or evidence that there has been a breach of security.

All pupils at KS2 and above will be provided with a username and password by the Network Manager who will keep an up-to-date record of pupils and their usernames.

The complexity (i.e. minimum standards) will be set with regards to the cognitive ability of the children.

1.4 Filtering and Monitoring

Internet access is filtered for all pupils. At Rainbow Forge Academy, if pupils become aware of any infringements or abuse of the Academy's filtering systems, they must report this immediately to their class teacher, Headteacher or DSL.

Pupils will not attempt to use any programmes or software that might allow them to bypass the filtering/security systems in place.

1.5 Using and Publishing Images and Videos Online

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, all Rainbow Forge Academy community need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or long term.

Guidance

Pupils will be advised about the risks associated with the taking, use, sharing, publication and distribution of images. They will be encouraged to recognise the risks attached to publishing their own image on the internet, e.g. on social networking sites.

Pupils will not take, use, share, publish or distribute images of others without their permission.

1.6 Managing Email

Pupils will use a provided email account for educational purposes.

Pupils will agree an Acceptable Use Agreement and will receive education regarding safe and appropriate email etiquette before access is permitted.

Whole-class or group email addresses will be used for communication outside of the setting**.**

1.7 Social Media

Expectations

The expectations regarding safe and responsible use of social media applies to all members of Rainbow Forge Academy community including pupils.

The term 'social media' may include (but is not limited to) blogs, wikis, social networking sites, forums, bulletin boards, online gaming, apps, video/photo sharing sites, chatrooms and instant messenger.
All members of Rainbow Forge Academy community are expected to engage in social media in a positive and responsible manner.

Pupils should not post or share content that may be considered threatening, hurtful or defamatory to others on any social media service.

We will control pupil access to social media while using any device and systems provided by Rainbow Forge Academy on site.

The use of social media during Academy hours for personal use is not permitted for pupils.

Concerns regarding the online conduct of any member of our Academy community on social media will be reported to the DSL without delay and be managed in accordance with our Anti-bullying, Allegations Against Staff, Code of Conduct, and Safeguarding policies.

Use of Social Media

Safe and appropriate use of social media will be taught to pupils as part of an embedded and progressive education approach via age-appropriate sites and resources.

We are aware that many popular social media sites are not permitted for use by children under the age of 13, or in some cases higher. As such, we will not create accounts for pupils under the required age as outlined in the services terms and conditions. See Appendix 7.

Any concerns regarding pupils' use of social media will be dealt with in accordance with existing policies, including Safeguarding, Anti-bullying, and Behaviour policies.

Concerns regarding pupils' use of social media will be shared with parents/carers as appropriate, particularly when concerning underage use of social media services and games.

Pupils will be advised:

- to consider the benefits and risks of sharing personal details or information on social media sites which could identify them and/or their location
- to only approve and invite known friends on social media sites and to deny access to others by making profiles private
- not to meet any online friends without a parent/carer or other appropriate adults' permission, and to only do so when a trusted adult is present
- to use safe passwords
- to use social media sites which are appropriate for their age and abilities
- how to block and report unwanted communications
- how to report concerns on social media, both within the setting and externally.

1.8 Mobile Technology – Use of Mobile Phones and Personal Devices

Rainbow Forge Academy recognises that personal communication through mobile technologies is part of everyday life for many pupils. Mobile technology needs to be used safely and appropriately within the Academy.

Expectations

All use of mobile technology, including mobile phones and personal devices such as tablets, games consoles and wearable technology, will take place in accordance with our policies, such as Safeguarding, Anti-bullying, Behaviour and Code of Conduct, and with the law.

Electronic devices of any kind that are brought onto site are the responsibility of the user.

As a result:

- Any mobile technology brought onto site by a pupil must be handed over to the office or Phase leaders to be stored out of children's reach until the end of the school day.
- all pupils are advised to take steps to protect their mobile phones or personal devices from loss, theft or damage; we accept no responsibility for the loss, theft or damage of such items on our premises
- we advise all pupils to use passwords/pin numbers to ensure that unauthorised calls or actions cannot be made on their phones or devices; passwords and pin numbers should be kept confidential and mobile phones and personal devices should not be shared
- mobile phones and personal devices are not permitted to be used in specific areas within the site or when on educational visits, such as changing rooms, toilets and swimming pools.
- Teachers will not direct children to use their mobile phone at any time during the school day.
- the sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the community; any breaches will be dealt with in line with the appropriate Trust or Academy policies
- all members of Rainbow Forge Academy community are advised to ensure that their mobile phones and personal devices do not contain any content which may be offensive, derogatory or would otherwise contravene our behaviour or child protection policies
- pupils will be educated regarding the safe and appropriate use of personal devices and mobile phones and will be made aware of boundaries and consequences
- if a pupil needs to contact his/her parents or carers, they will be allowed to use an Academy phone
- parents are advised to contact their child via the Academy office
- mobile phones and personal devices must not be taken into examinations
- pupils found in possession of a mobile phone or personal device during an exam will be reported to the appropriate examining body, this may result in the withdrawal from either that examination or all examinations
- if a pupil breaches the policy, the phone or device will be confiscated and held in a secure place and returned to the pupil or parents/carers at the end of the day
- staff may confiscate a pupil's mobile phone or device if they believe it is being used to contravene our Safeguarding, Behaviour or Anti-bullying policies
- searches of mobile phone or personal devices will be carried out in accordance with our procedures and in line with the DfE 'Searching, Screening and Confiscation' guidance https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1091132/Searching__Screening_and_Confiscation_guidance_July_2022.pdf
- pupils' mobile phones or devices may be searched by a member of the leadership team, with the consent of the learner or a parent/carer. Content may be deleted, or requested to be deleted, if it contravenes our policies
- if there is suspicion that material on a pupil's personal device or mobile phone may be illegal, or may provide evidence relating to a criminal offence, the device will be handed over to the police for further investigation. Staff members must be careful in carrying this out. Should a pupil have illegal material and a staff members views this, the staff member would be liable for prosecution should they view the material on the device. If the Academy suspects a mobile device of a pupil contains illegal material, the police should be informed so that it can be dealt with appropriately.

1.9 Concerns About Online Behaviour and/or Welfare

All concerns about pupils will be recorded in line with our Safeguarding policy. The DSL (or deputy) will be informed of all online safety concerns involving safeguarding or child protection risks.

Rainbow Forge Academy recognises that while risks can be posed by unknown individuals or adults online, pupils can also abuse their peers; all online child-on-child abuse concerns will be responded to in line with our Safeguarding and Behaviour policies.

The DSL (or deputy) will ensure that online safety concerns are escalated and reported to relevant partner agencies in line with local policies and procedures.

Appropriate sanctions and/or pastoral/welfare support will be offered to pupils as appropriate. Civil or legal action will be taken if necessary.

We will inform parents/carers of online safety incidents or concerns involving their child, as and when required.

National links and resources for pupils

- Childnet: www.childnet.com
    - Step Up Speak Up – Online Sexual Harassment Guidance: www.childnet.com/resources/step-up-speak-up/guidance-and-training-for-schools-and-professionals
    - Cyberbullying Guidance: www.childnet.com/resources/cyberbullying-guidance-for-schools

- Internet Matters: www.internetmatters.org

- NSPCC: www.nspcc.org.uk/onlinesafety
    - ChildLine: www.childline.org.uk

Net Aware: www.net-aware.org.uk

Part 2 – Staff/Adults

2.1 Roles and Responsibilities

The Headteacher, Jane Loader, and DSL, Nina Sneddon, have responsibility for online safety. **While activities of the DSL may be delegated to an appropriately trained deputy, overall, the ultimate lead responsibility for safeguarding and child protection, including online safety remains with them**.

Rainbow Forge Academy recognises that all members of the community have important roles and responsibilities with regards to online safety.

The Leadership and Management Team will:

- create a culture that incorporates online safety throughout all elements of Academy life
- ensure that online safety is viewed as a safeguarding issue and that practice is in line with national and local recommendations and requirements
- implement appropriate and up-to-date policies regarding online safety, which address the acceptable use of technology, child-on-child abuse, use of social media and mobile technology.
- Work with technical staff and L.E.A.D. IT support to ensure that suitable and appropriate filtering and monitoring systems are in place
- support the DSL and any deputies by ensuring they have enough time and resources to carry out their responsibilities
- ensure robust reporting channels are in place for the whole community to access regarding online safety concerns
- undertake appropriate risk assessments regarding the safe use of technology on site
- audit and evaluate online safety practice to identify strengths and areas for improvement
- ensure that staff, pupils and parents/carers are proactively engaged in activities which promote online safety
- support staff to ensure that online safety is embedded within a progressive whole setting curriculum which enables all pupils to develop an appropriate understanding of online safety.

The DSL will:

- act as a named point of contact within the setting on all online safeguarding issues
- liaise with other members of staff, such as pastoral support staff, IT technicians, network managers and the SENCO on matters of online safety
- ensure appropriate referrals are made to relevant external partner agencies, as appropriate
- work alongside the Safeguarding team and SLT to ensure online safety is recognised as part of the Academy safeguarding responsibilities, and that a coordinated whole Academy approach is implemented
- access regular and appropriate training and support to ensure they understand the unique risks associated with online safety and have the relevant and up-to-date knowledge required to keep pupils safe online.
- access regular and appropriate training and support to ensure the Academy recognises the additional risks that pupils with SEN and disabilities (SEND) face online
- ensure all members of staff receive regular, up-to-date and appropriate online safety training and information as part of their induction and child protection training
- keep up to date with current research, legislation and trends regarding online safety and communicate this with the community, as appropriate

- work with staff to coordinate participation in local and national events to promote positive online behaviour, such as a Safer Internet Day
- ensure that online safety is promoted to parents, carers and the wider community through a variety of channels and approaches, including workshops, training and individual support
- maintain records of online safety concerns, as well as actions taken, as part of the settings safeguarding recording mechanisms, relating to both adults and pupils
- monitor online safety incidents to identify gaps and trends and use this data to update the education response and Academy policies and procedures
- report online safety concerns, as appropriate, to L.E.A.D. IT, Rainbow Forge Academy senior leadership team and the Governing Body
- work with the Trust, L.E.A.D. IT and the leadership team to review and update Online Safety policies on a regular basis (at least annually) with stakeholder input
- meet regularly with the school IT technician and the governor with a lead responsibility for safeguarding and/or online safety.

It is the responsibility of all members of staff to:

- read and adhere to the Online Safety policy and Acceptable Use of Technology Agreements
- understand that sanctions may apply for breaches of acceptable use, which may include following Trust disciplinary procedures
- take responsibility for their own use of new technologies, making sure that they use technology safely, responsibly and legally
- take responsibility for the security of IT systems and the electronic data they use or have access to
- model good practice, in line with policy, when using technology with pupils
- maintain a professional level of conduct in their personal use of technology, both on and off site
- embed online safety education in curriculum delivery wherever possible
- have an awareness of a range of online safety issues and how they may be experienced by the pupils in their care
- identify online safety concerns and take appropriate action by following the Academy Safeguarding policies and procedures
- know when and how to escalate online safety issues, including reporting to the DSL and signposting pupils and parents/carers to appropriate support, internally and externally
- take personal responsibility for professional development in this area
- where appropriate, contribute to the development of our Online Safety policies
- ensure that any IT equipment taken from the Academy site is properly managed and kept securely. Ensure no overnight storage of IT equipment in cars
- ensure any data covered by GDPR is secure and a risk assessment undertaken as to why any personal data of staff or pupils has been removed from the school or hub site
- access to confidential Trust or Academy online databases and paper files should be permitted where access is required on a regular basis and is integral to the purpose of the role in question. Any access should be directly related to work matters and comply with the relevant data retrieval procedures.

2.2 Education and Engagement

We will:

- provide and discuss the Online Safety policy and procedures with all members of staff as part of induction
- provide up-to-date and appropriate online safety training (at least annually) for all staff which is integrated, aligned and considered as part of our overarching safeguarding approach.

- Staff training covers the potential risks posed to pupils (content, contact and conduct) as well as our professional practice expectations.
- Build on existing expertise by provide opportunities for staff to contribute to and shape our online safety approaches, including curriculum, policies and procedures.
- Make staff aware that our IT systems are monitored, and that activity can be traced to individual staff and pupils. Staff will be reminded to behave professionally and in accordance with our policies when accessing our systems and devices.
- Make staff aware that their online conduct, including personal use of social media, can have an impact on their professional role, reputation and could result in disciplinary procedures.
- Highlight useful educational resources and tools which staff could use with pupils.
- Ensure all members of staff are aware of the procedures to follow regarding online safety concerns involving pupils, colleagues or other members of the community.

2.3 Reducing Online Risks

Rainbow Forge Academy recognises that the internet is a constantly changing environment with new apps, devices, websites and material emerging at a rapid pace.

- We will:
  - regularly review the methods used to identify, assess and minimise online risks
  - examine emerging technologies for educational benefit and undertake appropriate risk assessments before their use in the Academy is permitted
  - ensure that appropriate filtering and monitoring is in place and take all reasonable precautions to ensure that access is appropriate
  - recognise that due to the global and connected nature of the internet, it is not possible to guarantee that unsuitable material cannot be accessed via our systems or devices and, as such, identify clear procedures to follow if breaches or concerns arise.

All members of the community are made aware of our expectations regarding safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos which could cause harm, distress or offence. This is clearly outlined in our Acceptable Use of Technology Agreements and highlighted through a variety of education and training approaches.

2.4 Safer Use of Technology

Classroom use

Rainbow Forge Academy uses a wide range of technology. This includes access to:

- computers, laptops, tablets and other digital devices

- internet, which may include search engines and educational websites learning platform/intranet
- email
- games consoles and other games-based technologies
- digital cameras, web cams and video cameras.

All setting-owned devices will be used in accordance with our Acceptable Use of Technology Agreement and procedures, and with appropriate safety and security measures in place. Adults must adhere to these procedures at all time.

Members of staff will always evaluate websites, tools and apps fully before use in the classroom or recommending for use at home.

The Academy adults will use appropriate search tools as identified following an informed risk assessment.

We will ensure that the use of internet-derived materials, by staff and pupils complies with copyright law and acknowledge the source of information.

Supervision of internet access and technology use will be appropriate to pupils' age and ability.

- **Early Years Foundation Stage and Key Stage 1**
  - Access to the internet will be by adult demonstration, with occasional directly supervised access to specific and approved online materials, which supports the learning outcomes planned for the pupil's age and ability.
- **Key Stage 2**
  - Pupils will use age-appropriate search engines and online tools.
  - Pupils will be directed by the teacher to online materials and resources which support the learning outcomes planned for the pupil's age and ability.

2.5 Password Security

Staff passwords:

- All staff will be provided with a username and password by the Network Manager/L.E.A.D. IT who will keep an up-to-date record of staff and their usernames.
- The password will be a minimum of eight characters long and must include three of the following – uppercase character, lowercase character, number, special characters.
- It will not include proper names or any other personal information about the user that might be known by others.
- The account will be 'locked out' following six successive incorrect log-on attempts
- Temporary passwords, e.g. used with new user accounts or when pupils have forgotten their passwords, shall be enforced to change immediately upon the next account log-on
- Passwords will not be displayed on screen and shall be securely hashed (use of one-way encryption).
- Passwords should be different for different accounts, to ensure that other systems are not put at risk if one is compromised and should be different for systems used inside and outside of the Academy and will be changed at least every 90 days.
- Passwords will not be re-used for six months, so passwords cannot be re-used passwords created by the same user.
- Passwords should be different for systems used inside and outside of the Academy.

Staff training/awareness
Members of staff will be made aware of the Academy's password protocols through the following:

- on induction
- through the Academy's Online Safety and Security policies
- pupils will be made aware of the Academy's password policy
- in lessons, a reminder will be given about the importance of not sharing passwords
- through the Acceptable Use Agreement.

2.6 Filtering and Monitoring

The filtering of internet content provides an important means of preventing pupils from accessing material that is illegal or inappropriate. The filtering system cannot, however, provide a 100% guarantee that it will do so, because the content on the web changes dynamically and new technologies are constantly being developed. Filtering is only one element in a larger strategy for online safety and acceptable use. Rainbow Forge Academy recognises that it is important that we have a filtering process to manage the associated risks and to provide preventative measures which are relevant to the situation in this Academy.

Staff and adults at Rainbow Forge Academy have a responsibility to report immediately to the Headteacher/L.E.A.D. IT/Network Manager any infringements of the Academy's filtering of which they become aware or any sites that are accessed, which they believe should have been filtered.

Staff/adults will not attempt to use any programmes or software that might allow them to bypass the filtering/security systems in place.

Differentiated internet access is available for staff and customised filtering changes are managed by the Academy and LEAD IT. Illegal content is filtered by the broadband or filtering provider, by actively employing the Internet Watch Foundation CAIC list and other illegal content lists. Filter content lists are regularly updated, and internet use is logged and monitored through SENSO. The monitoring process alerts the Academy to filtering breaches, which are then acted upon. There is a clear route for reporting and managing changes to the filtering system. Where personal mobile devices are allowed internet access through the Academy network, filtering will be applied that is consistent.

2.7 Managing the Safety of the Academy Website

We will ensure that information posted on our website meets the requirements as identified by the DfE.
We will ensure that our website complies with guidelines for publications including accessibility, data protection, respect for intellectual property rights, privacy policies and copyright.

Staff or pupils' personal information will not be published on our website; the contact details on the website will be our setting address, email and telephone number.

The administrator account for our website will be secured with an appropriately strong password.

We will post appropriate information about safeguarding, including online safety, on our website for members of the community.

2.8 Using and Publishing Images and Videos Online

When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. They will be encouraged to recognise the risks attached to publishing their own image on the internet, e.g. on social networking sites.
In accordance with guidance from the Information Commissioner's Office, parents/carers must not take photo's or videos of their child at academy events. Rainbow Forge academy staff will take photos and videos of events such as school performances and share them directly with parents or through our secure video sharing channels. To respect everyone's privacy and in some cases protection, these images should not be published or made publicly available on social networking sites, nor should parents or carers comment on any activities involving other pupils in the digital or video images.

Staff can take digital/video images to support educational aims, but will follow Academy procedures concerning the sharing, distribution and publication of those images. Those images should only be taken on Academy equipment; **the personal equipment of staff must not be used for such purposes**. Photos should be uploaded to the secure staff shared drive and images erased from any portable devices.

Care will 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.

Photographs published on our website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.

Staff will not use pupils' full names anywhere on a website or blog, particularly in association with photographs.

Staff must obtain written permission from parents or carers before photographs of pupils are published on the Academy website or social media channels (e.g. Facebook and Twitter).

Pupils' work will only be published with the permission of the pupil and parents or carers.

2.9 School and Staff Email

All members of staff are provided with an email address to use for all official work-related communication. Staff are required to use that email address for all Academy communication. **The use of personal email addresses by staff for any official business is not permitted.**

Access to our email systems will always take place in accordance with data protection legislation and in line with other policies, including the Confidentiality, Acceptable Use Agreements and the Code of Conduct Policy.

Staff must ensure any electronic communication which contains sensitive or personal information will only be sent using secure and encrypted email when being sent outside of the Trust. Internal emails do not need additional encryption.

Setting email addresses and other official contact details will not be used to set up personal social media accounts.

Members of the community will immediately tell the Headteacher and L.E.A.D. IT if they receive offensive communication, and this will be recorded in our safeguarding files/records (MyConcern).

2.10 Social Media

Expectations

The expectations regarding safe and responsible use of social media applies to all members of Rainbow Forge Academy community, staff and pupils. All members of Rainbow Forge Academy community are expected to engage in social media in a positive and responsible manner.

The term social media may include (but is not limited to) blogs, wikis, social networking sites, forums, bulletin boards, online gaming, apps, video/photo sharing sites, chatrooms and instant messenger.

All members of our community should not post or share content that may be considered threatening, hurtful or defamatory to others on any social media service.

We will control access to social media while using device and systems provided by Rainbow Forge academy on site.

The use of social media during Academy hours for personal use is not permitted for staff.

Concerns regarding the online conduct of any member of our Academy community on social media will be reported to the DSL without delay and be managed in accordance with our Anti-bullying, Allegations Against Staff, Code of Conduct and Safeguarding policies.

Use of social media

Academy staff will ensure that:

- no reference should be made in social media to pupils, parents/carers or Academy staff. Social media includes Facebook, LinkedIn, Twitter, WhatsApp, YouTube and all other networking sites, including blogs. The exception to this will be where the senior leadership team agree that a post can be made to promote the Academy and its pupils. Staff members must receive written agreement that such a post can be made. SLT will vet the posts to ensure they are acceptable and in line with existing Academy policies. See clause 8.4
- staff do not post or communicate disparaging or defamatory statements using social media or otherwise about:
    - our employees
    - our governors
    - our pupils and their parents/carers
    - our suppliers, agents and contractors
    - our Trustees
    - or statements that could be construed as being damaging or detrimental to the reputation of the Academy and/or the Trust
- staff do not engage in disparaging online discussion on personal or professional matters relating to members of the Academy community. This includes the use of WhatsApp groups or other social media sites

- staff are personally responsible for what they communicate via social media and that what they publish might be read by an audience wider than they intended
- that any social media communication is shared on their own behalf and does not appear to be linked with the Academy in any way
- personal opinions will not be attributed to the Academy or Trust
- security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information
- any electronic or text communication should be conducted through the Academy's communication systems
- staff do not have any present pupils or those that have left less than six years ago as 'friends', except relatives. However, if there is a legitimate reason for such communication, such as involvement with relevant clubs such as Scouts, Youth Club or Football, then this should be declared to the Headteacher and a copy of that organisation's Safeguarding policy should be provided
- the expectations apply whether or not social media is accessed using Academy facilities and equipment or equipment belonging to staff personally and to the use of social media for both Academy and personal purposes, whether or not during working hours or otherwise
- the Academy's use of social media for professional purposes will be checked regularly by the online safety coordinator and L.E.A.D. IT to ensure compliance with data protection, Online Safety and Safeguarding policies.

Unsuitable/inappropriate activities

Rainbow Forge Academy believes that the activities referred to in the following section would be inappropriate in an Academy context and that users, as defined below, will not engage in these activities in our Academy or outside when using Academy equipment or systems.

The Academy policy restricts usage as follows:

User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post,	Child sexual abuse images – The making, production or distribution of indecent images of children – contrary to The Protection of Children Act 1978					x

download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	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 the UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) – contrary to the Public Order Act 1986					x
	Pornography				x	
	Promotion of any kind of discrimination				x	
	Threatening behaviour, including promotion of physical violence or mental harm				x	
	Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the Academy or brings the Academy into disrepute				x	
Using Trust or Academy systems for personal gain, e.g. to run a private business or accessing information for non-work-related matters					x	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the Academy					x	
Infringing copyright					x	
Revealing or publicising confidential or proprietary information (e.g. financial/personal information, databases, computer/network access codes and passwords)					x	
Creating or propagating computer viruses or other harmful files					x	
Unfair usage (downloading/uploading large files that hinders others in their use of the internet)					x	
Online gaming (educational)					x	
Online gaming (non-educational)					x	
Online gambling					x	
Online shopping/commerce					x	
File sharing					x	

Use of social media – if not for the purpose of disparaging the Academy, colleagues, pupils of their families		x		x	
Use of messaging apps – if not for the purpose of disparaging the Academy, colleagues, pupils of their families		x			
Use of video broadcasting, e.g. YouTube – if not for the purpose of disparaging the Academy, colleagues, pupils of their families		x			

Official use of social media

Rainbow Forge Academy's official social media channels are:
https://www.facebook.com/profile.php?id=100089070624715

https://twitter.com/rainbowforgeaca

The official use of social media sites by Rainbow Forge Academy Academy only takes place with clear educational or community engagement objectives and with specific intended outcomes. Posts on these sites will only be at the discretion of the Headteacher and senior leadership team and Trust-approved social media contractors.

The official use of social media as a communication tool has been formally risk assessed and approved by the Head teacher.

Official social media channels have been set up as distinct and dedicated accounts for official educational or engagement purposes only.

Official social media use will be conducted in line with existing policies, including but not limited to Anti-bullying, Data Protection (GDPR), Confidentiality and Safeguarding.

All communication on official social media platforms by staff on behalf of the setting will be clear, transparent and open to scrutiny.

Parents/carers and pupils will be informed of any official social media use, along with expectations for safe use and action taken to safeguard the community.

Parents/carers will be informed of any official social media use with pupils; written parental consent will be obtained, as required.

We will ensure that any official social media use does not exclude members of the community who are unable or unwilling to use social media channels.

2.11 Streaming Media and Related Sites

'Streaming' is the method for which media content, most commonly video and audio, is delivered to an end-user. The media is stored on one computer or server and, via the Internet, played back on another. Streaming media is not downloaded and stored on the receiving computer as a whole file, but is typically viewed on demand via a web page. YouTube and Vimeo are examples of popular streaming media websites.

L.E.A.D. Academy Trust recognises that teaching can be enriched by the use of streaming media in the classroom. However, there are many identified risks associated with this type of content.

As a member of staff using streaming media in the classroom you will be expected to adhere to the following guidelines:

Acceptable Use

The primary purpose for using streaming media is to enhance teaching and learning within the school. Streaming Media must only be used for legitimate teaching purposes, personal use is prohibited.

Media content should be viewed from start to finish and a full assessment made of its suitability for the intended audience. The content should be considered in the same way that you would consider any other resources used in your classroom.

Content must be assessed away from the view and earshot of students, preferably in a staff room or similar. Many classroom PC's are connected to interactive whiteboards and projectors, and may be configured for whole class display.

This must be considered when reviewing content.

Where a resource is deemed appropriate for use, it is recommended that it is downloaded and saved for future use. This will prevent any issues with online content being removed or changed. Separate tools are required to download streaming media to a PC, and examples are available on the Intranet.

If it is not possible to download the resource then the video should be viewed prior to each use, to ensure it remains suitable for the intended purpose.

Unacceptable Use

It is deemed inappropriate to view, create, access, download or publish material that is:

- Pornographic or Adult
- Racist, offensive, or derogatory
- Obscene
- Bullying
- Violent
- Fraudulent
- Likely to cause harassment to others
- Confidential
- Prejudicial to the school's or Council's best interests
- Not relevant to the business of the school or Council
- Likely to irritate or waste time of others
- Likely to breach copyright

It is accepted that the teaching of certain subjects may present the need to use resources that could fall into one or more of the above categories. In such situations it is expected that the subject matter is presented in context; in a sensitive; balanced manner; and is appropriate for the age of the intended audience.

It is also expected that any home / school contracts regarding religion, sex education, parental wishes etc are considered when selecting media content.

2.12 Mobile Technology – Use of Mobile Phones and Personal Devices

Rainbow Forge Primary Academy recognises that personal communication through mobile technologies is part of everyday life for many pupils, staff and parents/carers. Mobile technology needs to be used safely and appropriately within the setting.

Members of staff will ensure that use of personal phones and devices takes place in accordance with the law, as well as, relevant policy and procedures, such as Confidentiality, Safeguarding, Data Protection and Acceptable Use policies.

Personal mobile devices should not be used during any face-to-face time with the pupils. Personal devices of any kind must be kept safely where pupils cannot access them.

Staff will be advised to:

- keep mobile phones and personal devices in a safe and secure place, for example a cupboard or drawer that the pupils do not have access to, during lesson time
- keep mobile phones and personal devices switched off or switched to 'silent' mode during lesson times and not on their person
- ensure that Bluetooth or other forms of communication, such as 'airdrop', are hidden or disabled during lesson times
- not use personal devices during teaching periods, unless permission has been given by the Headteacher such as in emergency circumstances
- ensure that any content bought onto site via mobile phones and personal devices is compatible with their professional role and expectations.

Members of staff are only permitted to use their own personal phones or devices for contacting parents/carers using the Dojo app. Phone calls to parents should be made on school phones, if this is not possible, staff must ensure their caller ID is witheld. Any pre-existing relationships which could undermine this will be discussed with the DSL (or deputy) and the Headteacher.

Staff will not use personal devices or mobile phones:

- to take photos or videos of pupils and will only use work-provided equipment for this purpose
- communicate directly with pupils and will only use work-provided equipment during lessons/educational activities.

If a member of staff breaches our policy, action will be taken in line with the Trust Disciplinary Policy, and where relevant, Managing Allegations Against Staff policy.

If a member of staff is thought to have illegal content saved or stored on a mobile phone or personal device, or have committed a criminal offence using a personal device or mobile phone, the police will be contacted and the LADO (Local Authority Designated Officer) will be informed in line with our Managing Allegations Against Staff policy.

Officially provided mobile phones and devices

Some members of staff will be issued with a work phone number and email address, where contact with pupils or parents/carers is required.

Rainbow Forge Primary Academy mobile phones and devices will be suitably protected via a passcode/password/pin and must only be accessed or used by members of staff.

Academy mobile phones and devices will always be used in accordance with the Acceptable Use of Technology Agreement and other relevant policies.

2.13 Responding to Online Safety Incidents

All members of Rainbow Forge Primary Academy community will be made aware of the reporting procedure for online safety concerns, including breaches of filtering, child-on-child abuse, including cyberbullying and youth-produced sexual imagery (sexting), online sexual violence and harassment, online abuse and exploitation and illegal content. Members of the community will respect confidentiality and the need to follow the official procedures for reporting concerns.

Pupils, parents and staff will be informed of our complaints procedure and staff will be made aware of the whistleblowing procedure.

We require staff, parents, carers and pupils to work in partnership with us to resolve online safety issues.

After any investigations are completed, the leadership will debrief, identify lessons learnt and implement any policy or curriculum changes, as required. If a member of staff has been dismissed for gross misconduct as a result of the misuse of devices or the internet, then the Headteacher will inform the Disclosure and Barring Service following the completion of the disciplinary process and in the case of a teacher, the TRA.

If we are unsure how to proceed with an incident or concern, the DSL (or deputy) will seek advice from the Trust. Where there is a concern that illegal activity has taken place, we will contact the police using 101, or 999 if there is immediate danger or risk of harm as appropriate. In such cases, Academy leaders will contact their HR Business Partner and their Director of Schools at the Trust and take advice on how to progress this matter internally.

If information relating to a specific incident or a concern needs to be shared beyond our community, for example, if other local settings are involved or the wider public may be at risk, the DSL and/or Headteacher will speak with the police and the LA Safeguarding team first, to ensure that potential criminal or child protection investigations are not compromised. The Trust DSL and the HR Business Partner will also be informed.

Concerns about staff online behaviour and/or welfare

Any complaint about staff misuse will be referred to the Headteacher, in accordance with our Managing Allegations Against Staff Policy.

Any allegations regarding a member of staff's online conduct will be discussed with the Local Authority Designated Officer (LADO and a Trust DSL).

Appropriate disciplinary, civil and/or legal action will be taken in accordance with the Staff Code of Conduct and Trust Disciplinary Procedure. Welfare support will be offered to staff as appropriate.

2.14 Procedure for Responding to Specific Online Safety Incidents

Online sexual violence and sexual harassment between children

Our Headteacher, DSL and appropriate members of staff have accessed and understood the DfE 'Sexual Violence and Sexual Harassment Between Children in Schools and Colleges' (2021) guidance and Part 5 of the latest guidance in

'Keeping Children Safe in Education'. Full details of our response to child-on-child abuse, including sexual violence and harassment can be found in our Safeguarding policy.

Rainbow Forge Academy recognises that sexual violence and sexual harassment between children can take place online. Examples may include:

- non-consensual sharing of sexual images and videos
- sexualised online bullying
- online coercion and threats
- 'up skirting', which typically involves taking a picture under a person's clothing without them knowing, with the intention of obtaining sexual gratification, or causing the victim humiliation, distress or alarm. It is a criminal offence
- unwanted sexual comments and messages on social media
- online sexual exploitation.

Adults will always respond to concerns regarding online sexual violence and sexual harassment between children, regardless of whether the incident took place on our premises or using our equipment.

If made aware of any concerns relating to online sexual violence and sexual harassment, we will:

- immediately notify the DSL (or deputy) and act in accordance with our Safeguarding and Anti-bullying policies
- if content is contained on pupils' personal devices, they will be managed in accordance with the latest DfE 'Searching, Screening and Confiscation at School' advice
- provide the necessary safeguards and support for all pupils involved, such as implementing safety plans, offering advice on blocking, reporting and removing online content, and providing appropriate counselling/pastoral support
- implement appropriate sanctions in accordance with our behaviour policy
- inform parents/carers, if appropriate, about the incident and how it is being managed
- if appropriate, make referrals to partner agencies, such as children's social care and/or the police
- if the concern involves children and young people at a different educational setting, the DSL will work in partnership with other DSLs to ensure appropriate safeguarding action is taken in the wider local community.

If a criminal offence has been committed, the DSL (or deputy) will discuss this with the police first to ensure that investigations are not compromised and review the handling of any incidents to ensure that best practice was implemented, and policies/procedures are appropriate.

Rainbow Forge Primary Academy recognises that the internet brings the potential for the impact of any sexual violence and sexual harassment concerns to extend further than the local community, and for a victim or alleged perpetrator to become marginalised and excluded by online communities.

We recognise the potential for repeat victimisation in the future if abusive content continues to exist somewhere online.

To help minimise concerns, we will ensure that all members of the community are made aware of the potential social, psychological and criminal consequences of online sexual violence and sexual harassment by implementing a range of age- and ability-appropriate educational methods as part of our curriculum.

We will ensure that all members of the community are aware of sources of support regarding online sexual violence and sexual harassment between pupils.

Youth-produced sexual imagery ('sexting')

Rainbow Forge Primary Academy recognises youth-produced sexual imagery (also known as 'sexting') as a safeguarding issue; all concerns will be reported to and dealt with by the Headteacher, DSL (or deputy).

We will follow the advice as set out in latest the non-statutory UKCIS guidance: 'Sharing Nudes and Semi-Nudes and the local guidance. Youth-produced sexual imagery or 'sexting' is defined as the production and/or sharing of sexual photos and videos of and by young people who are under the age of 18. It includes nude or nearly nude images and/or sexual acts. It is an offence to possess, distribute, show and make indecent images of children. This includes pupils themselves taking pictures and/or sending these images to others. The Sexual Offences Act 2003 defines a child, for the purposes of indecent images, as anyone under the age of 18. The process for managing any incidents of sexting in our Academy will be in line with Government guidance found here in Part 2 of the document 'Sharing Nudes and Semi-Nudes' https://ineqe.com/wp-content/uploads/2021/01/UKCIS_sharing_nudes_and_semi_nudes_advice_for_education_settings_V2.pdf

Safer Working Practices provides further guidance on managing indecent images:

- *'In the event of any indecent images of children or unsuitable material being discovered on a device the equipment should not be tampered with in any way. It should be secured and isolated from the network, and the DO contacted without delay. Adults should not attempt to investigate the matter or evaluate the material themselves as this may lead to a contamination of evidence and a possibility that they will be at risk of prosecution themselves.'*

Rainbow Forge Primary Academy will ensure that all members of the community are made aware of the potential social, psychological and criminal consequences of creating or sharing youth-produced sexual imagery by implementing preventative approaches, via a range of age- and ability-appropriate educational methods. Please see the safeguarding progression map and PSHE planning on the academy website.

We will ensure that all members of the community are aware of sources of support regarding the taking and sharing of youth-produced sexual imagery. For example sharing information for parents via the safeguarding termly newsletter.

We will respond to concerns regarding youth-produced sexual imagery, regardless of whether the incident took place on site or using setting-provided or personal equipment. See below for details.

Step 1 – Disclosure by a student

Sexting disclosures will follow the normal safeguarding practices and protocols (see Safeguarding policy) and a member of the Safeguarding team will be involved as soon as possible.

A pupil is likely to be very distressed, especially if the image has been circulated widely and if they do not know who has shared it, seen it or where it has ended up. They will need emotional support during the disclosure and after the event. They may need immediate protection or a referral to police or social services; parents should be informed as soon as possible (police advice permitting).

The following questions will help staff decide upon the best course of action:

- Is the student disclosing about themselves receiving an image, sending an image or sharing an image?
- What sort of image is it? Is it potentially illegal or is it inappropriate?
- Are the Academy Child Protection and Safeguarding policies and practices being followed?
- How widely has the image been shared and is the device in their possession?
- Is it an Academy device or a personal device?
- Does the student need immediate support and/or protection?
- Are there other pupils and/or young people involved?
- Do they know where the image has ended up?

Step 2 – Searching a device – what are the rules?

This policy allows for a device to be confiscated and securely stored if there is reason to believe it contains indecent images or extreme pornography. In 'Sharing Nudes and Semi-Nudes – Responding to Incidents and Safeguarding Young People' Part 2, guidance for carrying out searches is outlined. Our Academy will follow this guidance. See below for brief notes of this guidance.

If it is decided that searching a mobile device is necessary, the following conditions will be implemented:

- the search will be conducted by the DSL or a member of the leadership team and **at least** one other person
- a member of the Safeguarding team **WILL** be present
- Rainbow Forge Primary Academy will (where possible) make sure that the search is conducted by a member of the same gender as the person being searched. However, if the image being searched for is likely to be of a different gender to the person 'in possession', then the device will only be viewed by a member of the same gender as the person whose image it is.

If any illegal images of a young person are found, the DSL/Headteacher will discuss this with the police.

The Association of Chief Police Officers (ACPO) advises that, as a general rule, it will almost always be appropriate to refer any incident involving 'aggravated' sharing of images to the police, whereas purely 'experimental' conduct may appropriately be dealt with without such referral, most particularly if it involves the young person sharing images of themselves.

'Experimental conduct' commonly refers to that shared between two individuals (e.g. girlfriend and boyfriend) with no intention to publish the images further.

Coercion is not a feature of such conduct, neither are requests for images sent from one person to multiple other young persons.

Any conduct involving, or possibly involving, the knowledge or participation of adults should always be referred to the police.

If an 'experimental' incident is not referred to the police, the reasons for this should be recorded on the Academy's safeguarding reporting system – 'MyConcern'.

Rainbow Forge Primary Academy will always put the young person first. We will not search the device if this will cause additional stress to the student/person whose image has been distributed. Instead, we will rely on the description by the young person, secure the device and contact the police.

Staff will never:

- search a mobile device even in response to an allegation or disclosure if this is likely to cause additional stress to the student/young person UNLESS there is clear evidence to suggest not to do so would impede a police inquiry
- print out any material for evidence
- move any material from one storage device to another.

Staff will always:

- inform and involve the Safeguarding team who will ensure that the DSL (or Deputy DSL) is able to take any necessary strategic decisions
- record the incident. The Safeguarding team employs a systematic approach to the recording of all safeguarding issues using MyConcern
- act in accordance with Academy Safeguarding procedures.

If there is an indecent image of a child on a website or a social networking site, then the DSL/Headteacher will report the image to the site hosting it and any other relevant agencies such as social care.

Under normal circumstances, the team will follow the reporting procedures on the respective website. However, in the case of a sexting incident involving a child or young person, where it may be felt that they may be at risk of abuse, the team will report the incident directly to CEOP/police www.ceop.police.uk/ceop-report, so that law enforcement can make an assessment, expedite the case with the relevant provider and ensure that appropriate action is taken to safeguard the child.

Step 3 – What to do and not do with the image (If the image has been shared across a personal mobile device):

Rainbow Forge Primary Academy will always confiscate and secure the device(s), and close down or switch the device off as soon as possible. This may prevent anyone removing evidence 'remotely'.

We will never:

- view the image, unless there is a clear reason to do so or view it without an additional adult present (this additional person does not need to view the image and certainly should not do so if they are of a different gender to the person whose image has been shared). The viewing of an image should only be done to establish that there has been an incident which requires further action see 'Sharing Nudes and Semi-Nudes – Responding to Incidents and Safeguarding Young People' for guidance send, share or save the image anywhere
- allow pupils to do any of the above.

If the image has been shared across the Academy network, a website or a social network, we at Rainbow Forge Primary Academy will always block the network to all users and isolate the image.

We will never:

- send or print the image
- move the material from one place to another
- view the image outside of the protocols in the Academy's Safeguarding and Child Protection policies and procedures.

Step 4 – Who should deal with the incident?

Often, the first port of call for a pupil is a class teacher. Regardless of who the initial disclosure is made to, they will act in accordance with the Academy Safeguarding policy, ensuring that a member of the DSL and a senior member of staff are involved in dealing with the incident.

The DSL (or in their absence the deputy DSL) will always record the incident on MyConcern. The Headteacher will also always be informed, usually by the DSL. There may be instances where the image needs to be viewed and this should be done in accordance with protocols.

Step 5 – Deciding on a response

Rainbow Forge Primary Academy recognises that there may be many reasons why a pupil has engaged in sexting – it may be a sexual exploration scenario, or it may be due to coercion.

We understand that it is important to remember that it won't always be appropriate to inform the police; this will depend on the nature of the incident. However, as an Academy, we know it is important that incidents are consistently recorded. It may also be necessary to assist the young person in removing the image from a website or elsewhere.

If indecent images of a young person are found, we will:

- act in accordance with the Safeguarding policy
- store the device securely
- the DSL will assist the staff member to carry out a risk assessment in relation to the young person
- the DSL will make a referral (where necessary).

The DSL will contact the police (if appropriate). Referrals may be made to social care. Where a crime may have thought to have taken place, the police are the first port of call.

Young people who have engaged in 'experimental sexting' which is contained between two persons will be referred to other external agencies for support and guidance. Those who are felt to be victims of 'sexting' will also be referred to social care at a point where the police feel that this will not impede an investigation.

The young person's key worker or support people in the Academy will put the necessary safeguards in place for the student, e.g. they may need counselling support or immediate protection.

The DSL or deputy DSL will inform parents and/or carers about the incident and how it is being managed.

Step 6 – Containment and prevention

The pupil involved in 'sexting' may be left feeling sensitive and vulnerable for some time. We recognise that they may will require monitoring by and support from a member of staff at the Academy. If there are cases where 'sexting' becomes widespread or there is thought to be the possibility of contagion, then the Academy will reinforce the need for safer 'online' behaviour using a variety of resources.

Other staff may need to be informed of incidents (but only on a need to know basis) and should be prepared to act if the issue continues or is referred to by other pupils. Rainbow Forge Primary Academy, its pupils and parents will be on high alert, challenging behaviour and ensuring that the victim is well cared for and protected. The pupil's parents will usually be told what has happened so that they can keep a watchful eye over the young person especially when they are online at home.

Creating a supportive environment for pupils in relation to the incident is very important.

Preventative educational programmes on sexting can be found on CEOP's advice-giving website: www.thinkunknow.co.uk and the South West Grid for learning have developed advice for young people at: www.swgfl.org.uk/sextinghelp

There is also a lot of support and guidance for staff, pupils and parent/carers at NSPCC: https://www.nspcc.org.uk/preventing-abuse/keeping-children-safe/sexting/

Legal position

At Rainbow Forge Primary Academy, we understand that it is important to be aware that young people involved in sharing sexual videos and pictures are committing a criminal offence. Specifically, crimes involving indecent photographs (including pseudo-images) of a person less than 18 years of age fall under Section 1 of the Protection of Children Act 1978 and Section 160 Criminal Justice Act 1988. Under this legislation, it is a crime to:

- take an indecent photograph or allow an indecent photograph to be taken
- make an indecent photograph (this includes downloading or opening an image that has been sent via email)
- distribute or show such an image
- possess with the intention of distributing images
- advertise and possess such images.

While we realise that any decision to charge individuals for such offences is a matter for the Crown Prosecution Service, it is unlikely to be considered in the public interest to prosecute children. However, pupils need to be aware that they may be breaking the law. Although unlikely to be prosecuted, children and young people who send or possess images may be visited by police and, on some occasions, media equipment could be removed. This is more likely if they have distributed images.

Crime recording

Where the police are notified of incidents of youth-produced sexual imagery they are obliged, under the Home Office Counting rules and National Crime Recording Standards, to record the incident on their crime systems. The incident will be listed as a 'crime' and the young person involved will be listed as a 'suspect'.
This is not the same as having a criminal record.

However, there have been concerns that young people could be negatively affected should that crime be disclosed, for example, on an enhanced Disclosure and Barring Service (DBS) check.

To mitigate this risk, the NSPCC has worked with the Home Office and the DBS and provided policing with a new way of recording the outcome of an investigation into youth-produced sexual imagery. This is called Outcome 21.

Outcome 21
Every 'crime' recorded on police systems must be assigned an outcome from a predefined list of outcome codes. As of January 2016, the Home Office launched a new outcome code (Outcome 21) to help formalise the discretion available to the police when handling crimes such as youth-produced sexual imagery.

Outcome 21 states:

Further investigation, resulting from the crime report, which could provide evidence sufficient to support formal action being taken against the suspect is not in the public interest. This is a police decision.

This means that even though a young person has broken the law and the police could provide evidence that they have done so, the police can record that they chose not to take further action as it was not in the public interest.

Online abuse and exploitation (including child sexual abuse and sexual or criminal exploitation)

Rainbow Forge Primary Academy recognises online abuse and exploitation, including sexual abuse and sexual or criminal exploitation, as a safeguarding issue and all concerns will be reported to and dealt with by the DSL (or deputy), in line with our Safeguarding policy.

Rainbow Forge primary Academy will ensure that all members of the community are aware of online child abuse and sexual or criminal exploitation, including the possible grooming approaches which may be employed by offenders to target pupils, and understand how to respond to concerns.

We will implement preventative approaches for online child abuse and exploitation via a range of age- and ability-appropriate education for pupils, staff and parents/carers.

We will ensure that all members of the community are aware of the support available regarding online child abuse and exploitation, both locally and nationally.

We will ensure that the 'Click CEOP' report button used to report online child sexual abuse is visible and available to pupils and other members of our community via the website.

If made aware of an incident involving online child abuse and/or exploitation, we will:

- act in accordance with our Safeguarding policies and the relevant local safeguarding partnership procedures
- store any devices containing evidence securely
- if appropriate, make a referral to children's social care and inform the police via 101, or 999 if a learner is at immediate risk
- carry out a risk assessment which considers any vulnerabilities of learner(s) involved, including carrying out relevant checks with other agencies
- inform parents/carers about the incident and how it is being managed and provide support and signposting, as appropriate
- provide the necessary safeguards and support for pupils, such as offering counselling or pastoral support
- review the handling of any incidents to ensure that best practice is implemented; leadership team will review and update any management procedures, where necessary.

We will respond to concerns regarding online abuse and exploitation, regardless of whether the incident took place on our premises or using setting provided or personal equipment.

Where possible and appropriate, pupils will be involved in decision-making. If appropriate, they will be empowered to report concerns themselves with support, for example if the concern relates to online sexual abuse via CEOP: www.ceop.police.uk/safety-centre/

If we are unclear whether a criminal offence has been committed, the DSL (or deputy) will obtain advice immediately through the Education Safeguarding team and/or police.

If made aware of intelligence or information which may relate to child sexual exploitation (on or offline), it will be passed through to the police by the DSL (or deputy).

If members of the public or pupils at other settings are believed to have been targeted, the DSL (or deputy) will seek advice from the police and/or the Education Safeguarding team before sharing specific information to ensure that potential investigations are not compromised.

Indecent images of children (IIOC)

Rainbow Forge Primary Academy will ensure that all members of the community are made aware of the possible consequences of accessing IIOC as appropriate to the age and ability.

We will respond to concerns regarding IIOC on our equipment and/or personal equipment, even if access took place off site.

We will seek to prevent accidental access to IIOC by using an Internet Service Provider (ISP) which subscribes to the Internet Watch Foundation (IWF) block list and by implementing appropriate filtering, firewalls and anti-spam software.

If we are unclear if a criminal offence has been committed, the DSL (or deputy) will obtain advice immediately through the police and/or the Education Safeguarding team.

If made aware of IIOC, we will:

- act in accordance with our Safeguarding policy and the relevant local safeguarding partnership procedures
- store any devices involved securely
- immediately inform appropriate organisations, such as the IWF and police.

If made aware that a member of staff or a learner has been inadvertently exposed to IIOC, we will:

- ensure that the DSL (or deputy) and L.E.A.D. IT are informed
- ensure that the URLs (webpage addresses) which contain the suspect images are reported to the IWF via www.iwf.org.uk
- ensure that any copies that exist of the image, for example in emails, are deleted
- report concerns, as appropriate to parents/carers.

If made aware that IIOC have been found on the setting provided devices, we will:

- ensure that the DSL (or deputy) and L.E.A.D. IT are informed

- ensure that the URLs (webpage addresses) which contain the suspect images are reported to the IWF via www.iwf.org.uk
- inform the police via 101 or 999 if there is an immediate risk of harm, and children's social care, as appropriate
- only store copies of images (securely, where no one else has access to them and delete all other copies) following a written request from the police
- report concerns, as appropriate to parents/carers.

If made aware that a member of staff is in possession of IIOC on Rainbow Forge Primary Academy-provided devices, we will:

- ensure that the Headteacher is informed in line with our Managing Allegations Against Staff policy
- inform the Local LADO, Trust DSL and other relevant organisations in accordance with our Managing Allegations Against Staff policy
- quarantine any devices until police advice has been sought.

Staff should take extreme care to ensure that children and young people are not exposed, through any medium, to inappropriate or indecent images.

There are no circumstances that will justify adults: making, downloading, possessing or distributing indecent images or pseudo-images of children (child abuse images). Accessing these images, whether using the setting's or personal equipment, on or off the premises, or making, storing or disseminating such material is illegal.

If IIOC are discovered at the establishment or on the Academy's or setting's equipment, an immediate referral should be made to the Designated Officer (DO) and the police contacted if relevant. The images/equipment should be secured and there should be no attempt to view or delete the images as this could jeopardise necessary criminal action. If the images are of children known to the school, a referral should also be made to children's social care in line with local arrangements.

Under no circumstances should any adult use school or setting equipment to access pornography. Personal equipment containing pornography or links to it should never be brought into or used in the workplace. This will raise serious concerns about the suitability of the adult to continue working with children and young people.

Staff should keep their passwords confidential and not allow unauthorised access to equipment.

Cyberbullying

Cyberbullying, along with all other forms of bullying, will not be tolerated at Rainbow Forge Primary Academy. Full details of how we will respond to cyberbullying are set out in our Anti-bullying policy.

Online hate

Online hate content, directed towards or posted by, specific members of the community will not be tolerated at Rainbow Forge Academy and will be responded to in line with existing policies, including Safeguarding, Anti-bullying and Behaviour policies.

All members of the community will be advised to report online hate in accordance with relevant policies and procedures. The police will be contacted if a criminal offence is suspected.

If we are unclear on how to respond, or whether a criminal offence has been committed, the DSL (or deputy) will obtain advice through the Education Safeguarding team, Trust DSL and/or the police.

Online radicalisation and extremism

As listed in this policy, we will take all reasonable precautions to ensure that pupils and staff are safe from terrorist and extremist material when accessing the internet on site.

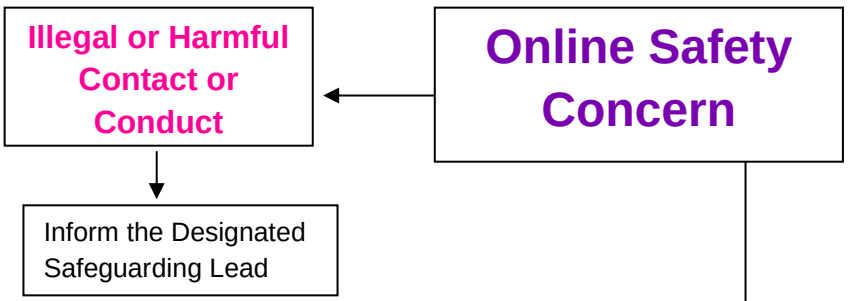
If we are concerned that a pupil or adult may be at risk of radicalisation online, the DSL (or deputy) will be informed immediately, and action will be taken in line with our safeguarding policy.

If we are concerned that a member of staff may be at risk of radicalisation online, the Headteacher will be informed immediately, and action will be taken in line with the Safeguarding and Allegations policies.

2.15 Breaches

At Rainbow Forge Primary Academy, we understand that we have a duty of care to provide a safe learning environment for pupils and staff. We could be held responsible, indirectly, for the acts of employees in the course of their employment. Staff members who harass, cyberbully, discriminate on the grounds of sex, race or disability or who defame a third party may render the Academy or Trust liable to the injured party. As a result, we will act to address any infringements of this policy with urgency.

Responding to an Online Safety Concern Flowchart



Key Local Contacts

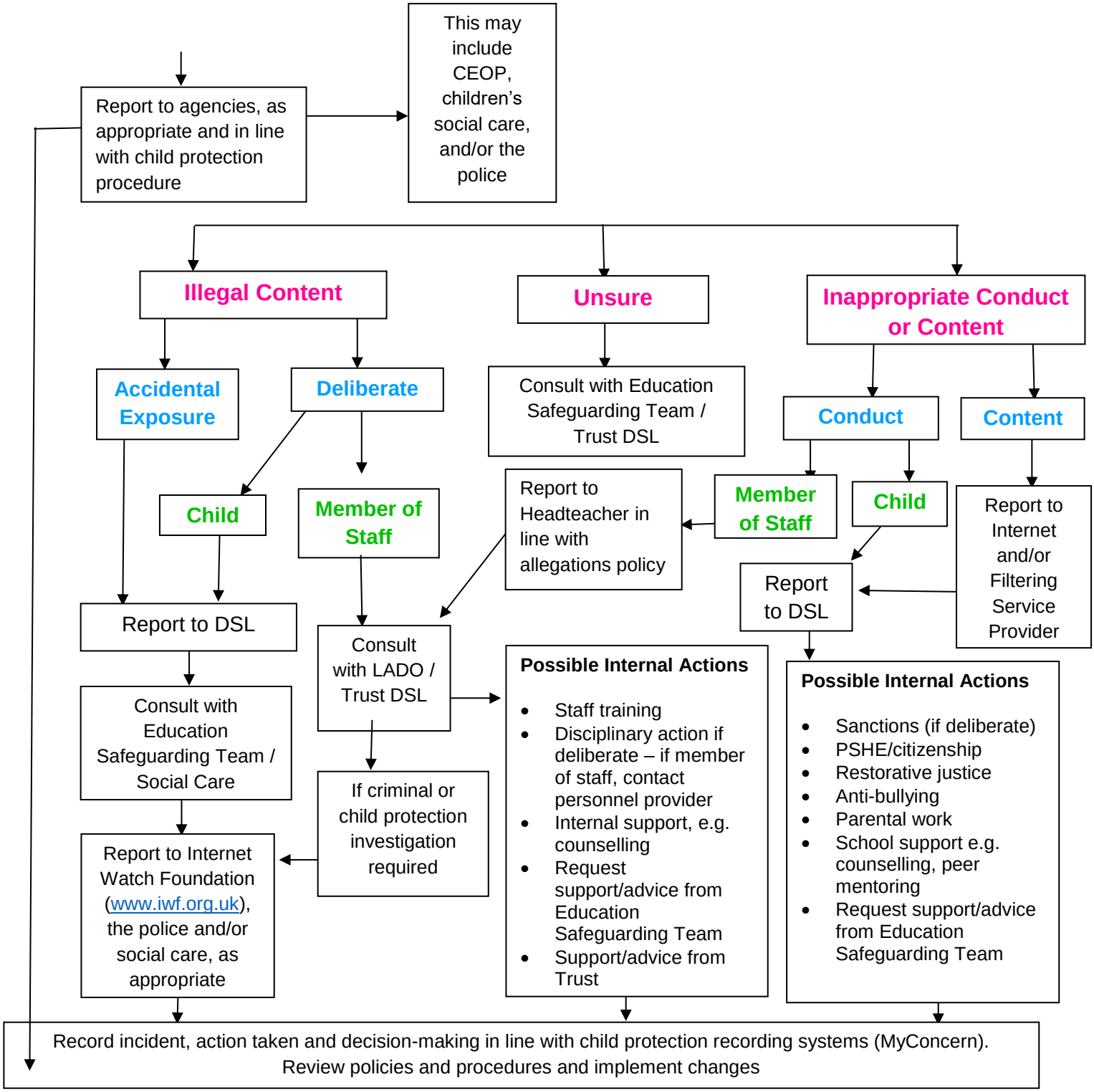
Designated Safeguarding Lead(s): Nina Sneddon (DSL) Jane Loader & Joanne Provines (DDSL)

Education Safeguarding Advisor: Emily Pickles 0114 205 2890/ 07554 582 917

Children's social care: Sheffield Safeguarding Hub 01142 734255

LADO: Andrew Adedoyin 01142 734855

Police: 101 or 999 if immediate risk of harm



National links and resources for staff/adults

- CEOP:
  - www.thinkuknow.co.uk
  - www.ceop.police.uk
- Internet Watch Foundation (IWF): www.iwf.org.uk

- UK Council for Internet Safety (UKCIS): www.gov.uk/government/organisations/uk-council-for-internet-safety

- UK Safer Internet Centre: www.saferinternet.org.uk
  - Professional Online Safety Helpline: www.saferinternet.org.uk/about/helpline
  - Report Harmful Content: https://reportharmfulcontent.com/

- Childnet: www.childnet.com
  - Step Up Speak Up – Online Sexual Harassment Guidance: www.childnet.com/resources/step-up-speak-up/guidance-and-training-for-schools-and-professionals
  - Cyberbullying Guidance: www.childnet.com/resources/cyberbullying-guidance-for-schools

- Internet Matters: www.internetmatters.org

- NSPCC: www.nspcc.org.uk/onlinesafety
  - ChildLine: www.childline.org.uk

Net Aware: www.net-aware.org.uk

- 360 Safe Self-Review tool for schools: www.360safe.org.uk

- www.lucyfaithfull.org

The Marie Collins Foundation: www.mariecollinsfoundation.org.uk

Safer Working Practices:

Guidance for Safer Working Practices Ma

Part 3 – Academy and L.E.A.D. Academy Trust (including L.E.A.D. IT)

3.1 Roles and Responsibilities

L.E.A.D. IT (also known as the Network Manager Technical staff) will:

- ensure that the Academy's technical infrastructure is secure and is not open to misuse or malicious attack
- ensure that the Academy meets required online safety technical requirements and any Local Authority online safety policy/guidance that may apply
- ensure staff/pupils may only access the networks and devices through a properly enforced password protection protocol, in which passwords are regularly changed
- make sure that they keep up to date with online safety technical information to effectively carry out their role and to inform and update others as relevant
- ensure that the use of the network, internet, remote access and email is regularly monitored in order that any misuse or attempted misuse can be reported to the Headteacher, IT Coordinator and online safety governor for investigation/action/sanction
- make sure that monitoring software/systems are implemented and updated as agreed in Academy policies
- provide technical support and perspective to the DSL and Academy leadership team, especially in the development and implementation of appropriate Online Safety policies and procedures
- implement appropriate security measures including SENSO as directed by the Trust/L.E.A.D. IT and/or the leadership team to ensure that the Academy IT infrastructure is secure and not open to misuse or malicious attack, while allowing learning opportunities to be maximised
- ensure appropriate technical support and access to our filtering and monitoring systems is given to the DSL and/or deputies to enable them to take appropriate safeguarding action when required.

3.2 Academy Technical Security – Passwords

Our Academy, alongside L.E.A.D. IT Services, is responsible for ensuring that the Academy infrastructure/network is as safe and secure as is reasonably possible and that:

- pupils can only access data to which they have right of access
- no user should be able to access another's files (other than that allowed for monitoring purposes within the Academy's policies)
- access to personal data is securely controlled in line with the Academy's personal data policy
- logs are maintained of access by pupils and of their actions while pupils of the system
- there is effective guidance and training for pupils
- there are regular reviews and audits of the safety and security of Academy computer systems
- there is oversight from senior leaders, and these have impact on policy and practice.

Academy technical systems are managed by L.E.A.D. IT Services, in ways that ensure that our Academy meets recommended technical requirements for example:

- there will be regular reviews and audits of the safety and security of Academy technical systems which will be reported to our academy each term for review at the governing body meetings.
- servers, wireless systems and cabling will be securely located and physical access restricted
- appropriate security measures are in place to protect the servers, firewalls, switches, routers, wireless systems, workstations, 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 appropriate and well-trained staff and L.E.A.D. IT
- all pupils have clearly defined access rights to Academy technical systems. Details of the access rights available to groups of pupils will be recorded by the Network Manager and will be reviewed, at least annually
- pupils will be made responsible for the security of their username and password, must not allow other pupils to access the systems using their log-on details and must immediately report any suspicion or evidence that there has been a breach of security
- the Network Manager is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations
- mobile device security and management procedures are in place (where mobile devices are allowed access to Academy systems)
- Academy technical staff regularly monitor and record the activity of pupils on the Academy technical systems and pupils are made aware of this in the AUA
- remote management tools are used by staff to control workstations and view users' activity
- an agreed policy is in place for the provision of temporary access of 'guests' (e.g. trainee teachers, supply teachers, visitors) onto the Academy system
- the Academy infrastructure and individual workstations are protected by up-to-date software to protect against malicious threats from viruses, worms, trojans etc.
- personal data cannot be sent over the internet or taken off the Academy site unless safely encrypted or otherwise secured.

The management of technical security will be the responsibility of the Network Manager.

3.3 Filtering and Monitoring

What is an internet filter?

An 'internet filter' is a type of software that controls the content users are exposed to when interacting with the internet.

Our approach to filtering

L.E.A.D. Academy Trust aims to provide a safe and secure educational environment in which our educators and students can utilise dynamic and collaborative online learning tools. One method that ensures our students are safe while learning is with the use of an internet filter. An internet filter is installed on all student computers. Our internet filtering software protects students from material that is deemed harmful or obscene. Our approach to internet filtering at L.E.A.D. Academy Trust is guided by the Keeping

Children Safe in Education guidance and legislation. At L.E.A.D. Academy Trust, our academic leaders collaborate with our technology department regarding decisions on what is blocked and what is allowed.

Our filter on Windows computers

The content filter we currently utilise on our Windows computers at L.E.A.D. Academy Trust is called iBoss. Below is some summary information on how this filter impacts the student experience.

Key web categories blocked:

- gambling, entertainment
- web proxies, file sharing
- private websites
- adult content
- chat apps
- social media (Twitter is allowed for staff; Facebook, Snapchat, Instagram are blocked).

Key web categories enabled:

- Education, Dictionary
- Business, Finance
- Art, Food, News.

Forced features:

- Safe Search Engine Search* (Safe Search is forced on and keywords not blocked by the search engine are further screened by iBoss).

- Google Clean Image: iBoss' dynamic filtering of Google images goes beyond standard Safe Search, ensuring the Acceptable Use of Technology policy is always enforced without limiting end-user access.

The filtering of internet content provides an important means of preventing pupils from accessing material that is illegal or is inappropriate. The filtering system cannot, however, provide a 100% guarantee that it will do so, because the content on the web changes dynamically and new technologies are constantly being developed. Filtering is only one element in a larger strategy for online safety and acceptable use. Rainbow Forge Primary Academy recognises that it is important that we have a filtering process to manage the associated risks and to provide preventative measures which are relevant to the situation in this Academy.

The responsibility for the management of the Academy's filtering process will be held by the Network Manager and L.E.A.D. IT. They will manage the Academy filtering and will keep records/logs of changes and of breaches of the filtering systems. These will be reported to our academy each term, retrospectively.

To ensure that there is a system of checks and balances and to protect those responsible, any changes to the Academy filtering service will:

- be logged in change control logs
- be reported to a second responsible person (the Headteacher)
- be reported to and authorised by a second responsible person prior to changes being made.

- Parents/carers will be informed of filtering breaches involving pupils.
- Any access to material believed to be illegal will be reported immediately to the appropriate agencies, such as the IWF, the police and/or CEOP.

3.4 Managing Personal Data Online

Personal data will be recorded, processed, transferred and made available online in accordance with General Data Protection Regulations and Data Protection legislation. See GDPR Policy for the Academy. Full information can be found in our information security policy which can be accessed via the school office.

3.5 Social Media

At Rainbow Forge Primary Academy, we understand that we have a duty of care to provide a safe learning environment for pupils and staff. We could be held responsible, indirectly, for the acts of employees in the course of their employment. Staff members who harass, cyberbully, discriminate on the grounds of sex, race or disability or who defame a third party may render the Academy or Trust liable to the injured party. As a result, we will act to address any infringements of this policy with urgency.

Rainbow Forge Primary Academy provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff, the Academy and the Trust through limiting access to personal information:

Training will include:

- 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.

3.6 Electronic and Press Communication

Rainbow Forge Primary Academy will ensure its website, electronic communication with parents, tweets and other posts will be vetted and supported by the Trust's communication and publicity arm, Engaging Education. Rainbow Forge Primary Academy understands that it may put itself or the Trust at reputational risk if it chooses not to engage with our communications experts.

Part 4 – Parents/Carers

4.1 Roles and Responsibilities

It is the responsibility of parents/carers to:

- read our Acceptable Use of Technology policies and encourage their children to adhere to them
- support our online safety approaches by discussing online safety issues with their children and reinforcing appropriate and safe online behaviours at home
- role model safe and appropriate use of technology and social media and abide by the Home-School Agreement and Acceptable Use of Technology policies
- seek help and support from the Academy or other appropriate agencies, if they or their child encounter online issues
- contribute to the development of our Online Safety policies
- use our systems and other IT resources, safely and appropriately
- take responsibility for their own awareness in relation to the risks and opportunities posed by the new and emerging technologies that their children access and use at home.

4.2 Education and Engagement

Rainbow Forge Primary Academy recognises that parents/carers have an essential role to play in enabling children and young people to become safe and responsible pupils of the internet and associated technologies.

We will build a partnership approach to online safety with parents/carers by:

- providing information and guidance on online safety in a variety of formats
- This will include offering specific online safety awareness workshops, sharing helpful links and information on the Dojo school story
- drawing their attention to our Online Safety policy and expectations in our newsletters and other external communication (such as letters and social media channels) as well as on our website
- requesting parents/carers read online safety information as part of joining our community, for example, within our Home-School Agreement
- requiring them to read our Acceptable Use policies and discuss the implications with their children.

4.3 Use and Publishing Images and Videos Online

Parents/carers will NOT take videos and digital images of their children at Academy events. This is to respect everyone's privacy and in some cases protection. Rainbow Forge Primary Academy will film key events such as the nativity and share the images on our safe you tube channel.

Parents/carers will not upload or add any images, videos, sounds or text that could upset, threaten the safety or offend any member of the Academy community.

4.4Mobile Technology – Use of Mobile Phones and Personal Devices

- Parents/Carers should ensure that mobile phones are not used inside the academy building unless under specific guidance of a member of staff.

- Visitors, including volunteers and contractors, who are on site for regular or extended periods of time are expected to use their mobile phones and personal devices in accordance with our AUA and other associated policies, including but not limited to Anti-bullying, Behaviour, and Safeguarding.
- Members of staff are expected to challenge parents/carers if they have concerns and inform the DSL (or deputy) or Headteacher of any breaches of our policy.

4.5 Concerns about Parent/Carer Online Behaviour and/or Welfare

Concerns regarding parents/carers behaviour and/or welfare online will be reported to the Headteacher or DSL (or deputy).The Headteacher or DSL will respond to concerns in line with existing policies, including but not limited to Safeguarding, Anti-bullying, Complaints, Allegations Against Staff, Home-School Agreements, Acceptable Use of Technology and Behaviour policies.

Civil or legal action will be taken if necessary.

Welfare support will be offered to parents/carers as appropriate.

National links and resources

- Parent Zone: https://parentzone.org.uk

- Parent Info: https://parentinfo.org

- NSPCC: www.nspcc.org.uk/onlinesafety
  - ChildLine: www.childline.org.uk

Net Aware: www.net-aware.org.uk

- 360 Safe Self-Review tool for schools: www.360safe.org.uk
- www.lucyfaithfull.org
- The Marie Collins Foundation: www.mariecollinsfoundation.org.uk
- Get Safe Online: www.getsafeonline.org

Part 5 – Visitors

5.1 Roles and Responsibilities

It is the responsibility of visitors to:

- read our acceptable use of technology agreements and to adhere to them
- role model safe and appropriate use of technology and social media and abide by Acceptable Use of Technology Agreement

- seek help and support from the Academy or other appropriate agencies, if they encounter online issues
- use our systems and other IT resources, safely and appropriately
- take responsibility for their own awareness in relation to the risks and opportunities posed by the new and emerging technologies.

5.2Mobile Technology – Use of Mobile Phones and Personal Devices

Visitors, including volunteers and contractors, should ensure that mobile phones are not used when in sight of the pupils. Volunteers should follow the same guidelines as staff and keep phones safely away from pupils when in classrooms. Contractors may need to call colleagues and this should be done in areas of the school where children do not enter, for example the site supervisors office.

- Appropriate signage and information are provided to inform parents/carers and visitors of expectations of use.
- Visitors, including volunteers and contractors, who are on site for regular or extended periods of time are expected to use their mobile phones and personal devices in accordance with our AUA and other associated policies, including but not limited to Anti-bullying, behaviour, and Safeguarding.
- Members of staff are expected to challenge visitors if they have concerns and inform the DSL (or deputy) or Headteacher of any breaches of our policy.

Appendices

Appendix 1

Pupil Acceptable Use Agreement

Early Years and Key Stage 1 (0–6)

- I only use the internet when an adult is with me.

- I only click on links and buttons online when I know what they do.
- I keep my personal information and passwords safe.
- I only send messages online which are polite and friendly.
- I know Rainbow Forge Primary Academy can see what I am doing online.
- I always tell a trusted adult if something online makes me feel unhappy or worried.
- I can visit www.thinkuknow.co.uk to learn more about keeping safe online.
- I know that if I do not follow the rules I will be given a reminder, warning and consequence.
- I have read and talked about these rules with my parents/carers.

Shortened version (for use on posters)

- I only go online with a grown-up.
- I am kind online.
- I keep information about me safe online.
- I tell a grown-up if something online makes me unhappy or worried.

Key Stage 2 (7–11)

Safe

- I only send messages which are polite and friendly.
- I will only post pictures or videos on the internet if they are appropriate, and if I have permission.
- I only talk with and open messages from people I know, and I only click on links if I know they are safe.
- I know that people I meet online may not always be who they say they are. If someone online suggests meeting up, I will immediately talk to an adult.

Trust

- I know that not everything or everyone online is honest or truthful.
- I will check content on other sources like other websites, books or with a trusted adult.
- I always credit the person or source that created any work, image or text I use.

Responsible

- I always ask permission from an adult before using the internet.
- I only use websites and search engines that my teacher has chosen.
- I use Rainbow Forge Primary Academy computers for schoolwork, unless I have permission otherwise.
- I do not use my own personal devices/mobile phone in school.
- I keep my personal information safe and private online.
- I will keep my passwords safe and not share them with anyone.
- I will not access or change other people's files or information.

- I will only change the settings on the computer if a teacher has allowed me to.

Understand

- I understand that the Academy internet filter is there to protect me, and I will not try to bypass it.
- I know that my use of Rainbow Forge Primary Academy devices/computers and internet access will be monitored.
- I have read and talked about these rules with my parents/carers.
- I can visit www.thinkuknow.co.uk and www.childline.org.uk to learn more about being safe online.
- I know that if I do not follow the Academy rules then I will be given a reminder, warning and consequence.

Tell

- If I am aware of anyone being unsafe with technology, I will report it to a teacher.
- I always talk to an adult if I'm not sure about something or if something happens online that makes me feel worried or frightened.
- If I see anything online that I shouldn't or that makes me feel worried or upset then I will minimise the page or shut the laptop screen and tell an adult straight away
-

Shortened KS2 version (for use on posters)

- I ask a teacher about which websites I can use.
- I will not assume information online is true.
- I know there are laws that stop me copying online content.
- I know I must only open online messages that are safe. If I'm unsure, I won't open it without speaking to an adult first.
- I know that people online are strangers and they may not always be who they say they are.
- If someone online suggests meeting up, I will always talk to an adult straight away.
- I will not use technology to be unkind to people.
- I will keep information about me and my passwords private.
- I always talk to an adult if I see something which makes me feel worried.

NB. These guidelines and posters should be adapted for pupils with SEND that effects their literacy or understanding.

Pupil Acceptable Use Agreement Form

Rainbow Forge Academy Acceptable Use Agreement – Pupil

I, with my parents/carers, have read and understood the Acceptable Use Agreement (AUA).

I agree to follow the AUA when:

Appendix 2

Acceptable Use Agreement forms for Parents/Carers

Parent/Carer Acknowledgement Form

Learner Acceptable Use Agreement: Rainbow Forge Primary Academy Parental Acknowledgment

1. I, with my child, have read and discussed Rainbow Forge Primary Academy learner acceptable use agreement (AUA). I understand that the AUA applies to the use of the internet and other related devices and services, inside and outside of the setting.

2. I am aware that any internet and IT use using Rainbow Forge Primary Academy equipment may be monitored for safety and security reason to safeguard both my child and the Academy systems. This monitoring will be proportionate and will take place in accordance with data protection, privacy and human rights legislation.

3. I understand that the Academy will take every reasonable precaution, including monitoring and filtering systems, to ensure my child will be safe when they use the internet and other associated technologies. I understand that the Academy cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.

4. I, with my child, am aware of the importance of safe online behaviour and will not deliberately upload or add any images, video, sounds or text that could upset, threaten the safety of or offend any member of the Academy community.

5. I understand that Rainbow Forge Primary Academy will contact me if they have concerns about any possible breaches of the AUA or have any concerns about my child's safety.

6. I will inform Rainbow Forge Primary Academy or other relevant organisations if I have concerns over my child's or other members of the Academy's communities' safety online.

7. I know that my child will receive online safety education to help them understand the importance of safe use of technology and the internet – both in and out of the Academy.

8. I will support Rainbow Forge Primary Academy's online safety approaches and will encourage my child to adopt safe use of the internet and other technology at home.

Child's Name…… Child's Signature …… (***if appropriate***)

Class…… Date…….

Parent's/Carer's Name…….....

Parent's/Carer's Signature…… Date…….

Parent/Carer Acceptable Use Agreement

1. I know that my child will be provided with internet access and will use a range of IT systems to access the curriculum and be prepared for modern life while at Rainbow Forge Primary Academy.
2. I am aware that pupils' use of mobile technology and devices, such as mobile phones**, is not** permitted at Rainbow Forge Primary Academy.
3. I am aware that any internet and technology use using Rainbow Forge Primary Academy equipment may be monitored for safety and security reasons, to safeguard both my child and the Academy systems. This monitoring will take place in accordance with data protection (including GDPR) and human rights legislation.
4. I understand that the Academy will take every reasonable precaution, including monitoring and filtering systems, to ensure that pupils are safe when they use the Academy internet and systems. I understand that Rainbow Forge Primary Academy cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.
5. I am aware that my child will receive online safety education to help them understand the importance of safe use of technology and the internet, both in and out of Rainbow Forge Primary Academy.
6. I have read and discussed this Rainbow Forge Primary Academy Pupil AUA with my child.
7. I will support Rainbow Forge Primary Academy's Safeguarding policies and will ensure that I appropriately monitor my child's use of the internet outside of the Academy and discuss online safety with them when they access technology at home.
8. I know I can seek support from the Academy about online safety, such as via the Rainbow Forge Primary Academy website, to help keep my child safe online at home.
9. I will support the Academy approach to online safety. I will role model safe and positive online behaviour for my child by sharing images, text and video online responsibly.
10. I, together with my child, will not deliberately upload or add any images, video, sounds or text that could upset, threaten the safety of or offend any member of the Academy community.
11. I understand that a partnership approach to online safety is required. If Rainbow Forge Primary Academy has any concerns about either my or my child's behaviour or safety online, then I will be contacted.
12. I understand that if I or my child do not abide by Rainbow Forge Primary Academy AUA, appropriate action will be taken. This could include sanctions being applied in line with the Academy policies and if a criminal offence has been committed, the police being contacted.
13. I know that I can speak to the Designated Safeguarding Lead, Nina Sneddon, my child's teacher, or the Headteacher if I have any concerns about online safety.

I have read, understood and agree to comply with this Rainbow Forge Primary Academy Parent/Carer Acceptable Use Agreement.

Child's Name…….. Class……

Parent's/Carer's Name…….....

Parent's/Carer's Signature…… Date…….

Appendix 3

Staff Acceptable Use Agreement

Context

This **Individual User Agreement** is intended to provide a framework for the use of L.E.A.D. Academy Trust ICT resources. It seeks to clarify the principles for acceptable use of ICT as L.E.A.D. Academy Trust.

Acceptable Use Agreement Forms for Staff

ICT is used throughout the Trust, both in administrative and learning contexts; however, there is an explicit recognition that it must be used responsibly in line with the Online Safety policy and Acceptable Use of Technology Agreement. It is a clear requirement of this policy that users utilise ICT within clear and acceptable guidelines. It is of equal importance that our community of users are themselves protected as far as is reasonably practicable from any potential harm that may result from unacceptable, uninformed and inappropriate use.

To facilitate the above, all users must:

- **take full responsibility for their own use of new technologies, making sure that they use technology safely, responsibly and legally**
- **report any concerns regarding use of technology by pupils, staff and parents/carers without delay to the DSL**
- **agree to abide by and follow 'acceptable use' through signing to say this agreement has been read**
- **understand and accept that sanctions may apply for breaches of acceptable use in line with the Online Safety policy and Acceptable Use of Technology Agreement and this agreement, which may include suspension, dismissal, or criminal prosecution.**

'Acceptable use' is treating equipment with care, ensuring it is secure and utilising it in a way that is not illegal or may bring either the individual or the Trust into disrepute. The policy considers appropriate use under different headings which seek (though not exhaustively) to clarify how equipment should be used within the context of a learning environment.

Key aspects

The information below covers the principles of use for key aspects of ICT at L.E.A.D. Academy Trust. The separate guidance information is to inform users of specific detail relating to use. This information may change very quickly and will be updated on a regular basis. This additional information is designed to clarify the policy. Random checks will be undertaken to ensure that users are complying with this policy.

1. Name:

Position:

Department:

Access rights: *[Insert the detailed access rights to be granted in terms of in GDPR-C DOC 9.1.2]* and levels of confidentiality the user is entitled to access.

User access request originated by: HR Department

[Date]

User access request approved by: Manager/Executive (generic/line)

[Date]

User access request approved by: *[Asset owner(s)]*

[Date]

User acceptance of access rights and responsibilities as set out in this agreement:

Signed and agreed by staff member:

[Date]

User access name allocated:

Email address allocated:

Data storage file allocated:

User access request processed IT Department

[Date]

1.1 I, *[ ],* accept that I have been granted the access rights defined in this agreement to those organisational information assets also identified in this agreement.

1.2 I understand and accept the rights which have been granted, I understand the business reasons for these access rights, and I understand that breach of them, and specifically any attempt to access services or assets that I am not authorised to access – including any attempts to read, copy, modify or remove any personal data without prior authorisation – may lead to disciplinary action and specific sanctions.

1.3 I also accept and will abide by L.E.A.D. Academy Trust's Internet AUA, its email policy and its Information Security Weakness and Event Reporting policy. I understand that failure to comply with this agreement, or the commission of any information security breaches, may lead to the invocation of L.E.A.D. Academy Trust's disciplinary policy.

1.4 I acknowledge that I have received adequate training in all aspects of my use of L.E.A.D. Academy Trust's systems and of my responsibilities under this agreement.
I acknowledge that files stored on the network is the property of L.E.A.D. Academy Trust.

1.5 I acknowledge that any sections of this document are also subject to Child Protection and Safeguarding policies.

1.6 I understand that L.E.A.D. Academy Trust has legal duties in respect of the safeguarding and protection of pupils. Staff are required by L.E.A.D. Academy Trust policy to divulge the contents of any communication that they become aware of, to the Head Teacher or other nominated Designated Safeguarding Lead, if, in their opinion, the content gives rise to any potential concern for a pupil's wellbeing. These communications may in turn be shared with other statutory bodies charged with child protection as required by law.

2. Passwords

2.1 My username and password will be issued in line with L.E.A.D. Academy Trust's procedure for authorising and issuing them.
2.2 I will change my initial temporary password at first log-on.
2.3 I will select and use passwords that are at least eight characters in length, are alpha-numeric, are not based on any easily guessable or memorable data such as names, dates of birth, telephone numbers etc., are not dictionary words and are free of consecutive identical all-numeric or all-alphabetic characters.
2.4 I will keep my password secret and will not under any conditions divulge it to or share it with anyone, nor will I write it down and leave it anywhere that it can easily be found by someone else or record it anywhere without having obtained the specific authorisation of the Information Security Manager to do so.
2.5 Passwords can be shared with ICT Support where needed.
2.6 I will not store my password in any automated log-on process.
2.7 I will change my password at intervals as required by L.E.A.D. Academy Trust, will not attempt to re-use passwords or use new passwords that are in a sequence, and will change my password more frequently if there is evidence of possible system or password compromise.
2.8 I will not use the same password for organisational and personal use.
2.9 Under no circumstances will I attempt to disguise or mask my identity.
2.10 I will not attempt to breach the technical safeguards set up to safeguard my network access.

3. Clear desk policy, screensavers and information reproduction

3.1 I understand that I am required to ensure that no confidential or restricted information (in paper or removable storage media format) is accessed or shared without a legitimate work-related reason or purpose. I confirm none of the afore mentioned are left on my desk, in my environs, or left in or near reproduction equipment (photocopiers, fax machines, scanners) when I am not in attendance and will ensure that such information is secured in line with L.E.A.D. Academy Trust's security requirements as set out in GDPR-C DOC 8.2.
3.2 I understand that I am required to ensure that no one is able to access my workstation when I am not in attendance and that I must have a password-protected screensaver that operates within 30 minutes of no activity or which I activate when I leave the workstation unattended.
3.3 I know that I am required to terminate active computer sessions when I have finished them and to log off (i.e. not simply turn off the computer screen) whenever I am finished working and that the workstation is to be protected by appropriate key locks when I am away from the building.
3.4 I accept that I am not allowed to use personal storage media, MP3 players, digital cameras and mobile phones with photographic capability.
3.5 I accept that I may only use L.E.A.D. Academy Trust's reproductive equipment (photocopiers, fax machines, scanners) for proper organisational purposes and that I will ensure that I will use facilities that are appropriate for the classification level of any information with which I am dealing.

4. Mobile devices

4.1 In line with the principles of the policy overall, any mobile device be utilised appropriately and responsibly.
4.2 It is the user's responsibility to ensure that no viruses are enabled through negligence. Any mobile device brought onto L.E.A.D. Academy Trust premises should be virus free and checked on a regular basis.

4.3 It is the responsibility of any user who uses a mobile device to ensure the security of stored data. Data must not be downloaded and copied from the network or attached machines unless you have the appropriate authority to do so.

4.4 All mobile devices should be password protected. L.E.A.D. Academy Trust reserves the right to refuse the ability to connect mobile devices to the L.E.A.D. Academy Trust network infrastructure, if it feels such equipment is being used in a way that puts the Trust systems and data at risk.

4.5 L.E.A.D. Academy Trust accepts no responsibility for the safety of any such equipment, and it is brought into Trust at the user's own risk.

5. Internet Use

5.1 Users of L.E.A.D. Academy Trust equipment should use the internet responsibly and proportionately. The internet is a rich resource base for learning; however, websites should be accessed with appropriate caution and should not detract from other key work tasks. If an inappropriate website is accessed by accident, this should be reported to a member of SLT who will then liaise with the Network Manager. Users must not access/use websites that are inappropriate (these include websites that are unlawful, obscene, of pornographic, abusive or adult material).

6. Use of Social Networking Websites and Online Forum:

6.1 Users are prohibited from using Trust equipment for accessing social networking sites or online forums not directly linked to educational purposes. Any use of these sites should not damage their personal standing or the standing of L.E.A.D. Academy Trust. Social networking sites invite users to participate in informal ways that can leave users open to abuse.

6.2 I will not create Academy-based social media accounts unless they are fully approved by the Headteacher and the Trust IT department.

6.3 I will not use social media in any form to bring the Academy or Trust into disrepute when sharing posts or messages.

7. Software

Users have a clear responsibility to ensure they do not jeopardise the integrity, performance or reliability of computer equipment, software, data, and other stored information. The integrity of the computer systems is put at risk if users do not take adequate precautions against malicious software.

7.1 I will ensure that no attempts are made to disable or override any of L.E.A.D. Academy Trust's installed software, including anti-malware software, firewalls and automatic updating services.

7.2 I accept that I may not download from the internet or install on any organisational computer or other device any software of any sort for which L.E.A.D. Academy Trust does not have a valid licence and that has not had the prior authorisation of the Director of IT. I recognise that this prohibition includes freeware, shareware, screensavers, toolbars and/or any other programs that might be available.

7.3 I recognise that L.E.A.D. Academy Trust's requirements in respect of the acceptable use of Microsoft Teams facilities and will abide by it.

8. Data control and legislation

8.1 I will obtain the written authorisation of the Data Protection Officer/GDPR Owner for the storage of any personal data (mine or anyone else's) on L.E.A.D. Academy Trust's computer systems.

8.2 I will ensure that I abide by any legal requirements in respect of my computer use, including privacy and data protection regulations.

9. Backup and information classification

9.1 I acknowledge that I am responsible for ensuring that all information on my workstation is correctly classified and labelled in line with the requirements of GDPR-C DOC 8.2. I will ensure that this requirement is complied with.

9.2 I acknowledge that I am responsible for backing up information on my workstation by periodically restarting my laptop to ensure updates take effect.

9.3 I understand that I am required to store all data on company network drives and L.E.A.D. Academy Trust SharePoint and that I may not store information on the C:Drive of my computer.

10. Maintenance and IT equipment (to include infrastructure)

ICT equipment is a valuable learning and administrative resource. All ICT equipment must be handled with care and respect.

10.1 I accept that I am responsible for the physical security of my workstation and will report any faults immediately to ICT Support.

10.2 I understand that I should not leave my IT equipment in my car unattended in the daytime or overnight.

11 Audit and security monitoring

11.1 During the six-monthly audits, a random selection of users from each school will take place to determine rules put in place are covered. Any user types that fail will mean further tests must be carried out on that school.

12. Email use

The following rules are required by law and are to be strictly adhered to. It is prohibited to:

12.1 Send objectionable material such as pornography and sexually explicit jokes.

12.2 Use L.E.A.D. Academy Trust email systems to engage in conduct that could be deemed illegal, immoral or unethical.

12.3 Send offensive or discriminatory messages based on race, age, disabilities, gender, sexual orientation, or religious or political beliefs or other basis that is protected under applicable law.

12.4 Use email to advertise or otherwise support unapproved or illegal activities.

12.5 Use email in any way that reflects poorly on L.E.A.D. Academy Trust name, reputation and image.

12.6 Exchange gossip about themselves or others, or rumours, exaggerated claims and unsubstantiated opinions relating to the Trust or individual employees.

12.7 Send or forward emails outside of the Trust with personal data, unless the contents are encrypted.

12.8 Respond to any email that asks for personal or corporate account information, passwords or similar information. It is likely to be a phishing attempt. Immediately delete it and report the email to ICT Support.

12.9 Send or forward emails with an attachment that knowingly contains a virus.

12.10 Forge or attempt to forge email messages.

12.11 Disguise or attempt to disguise your identity when sending mail.

12.12 Send email messages using another person's email account without the individual's or line management's knowledge or permission.

12.13 The L.E.A.D. Academy Trust email system is to be used for educational and business communication. Therefore, the sending of personal emails, chain letters, junk mail, jokes and executables is prohibited.

12.14 All messages and files distributed via the email system, servers and transport mechanisms are L.E.A.D. Academy Trust property and there should be no expectation of any privacy in any such messages or files.

12.15 It is prohibited to use personal email when it interferes with job responsibilities such as face-to-face teaching or other duties such as dinner duties or playtime duties. This includes spending what is deemed to be disproportionate, unreasonable or unwarranted time on email activities.

12.16 All email header information, content and attachments are copied and archived into a separate location from the email server for an indefinite period and can only be deleted by authorised personnel.

12.17 All emails are recoverable and can be used as evidence, if appropriate.

12.18 If you receive any offensive, unpleasant, harassing or intimidating messages via the email, you are requested to inform the ICT Team immediately. It is important that we trace such emails as quickly as possible.

12.19 Employees who feel that they have cause for complaint because of email communications should raise the matter initially with their immediate Line Manager. If necessary, the complaint can be dealt with under the grievance procedure.

Further notes on email etiquette

Writing emails:

- All email messages must be appropriate and professional. Write well-structured emails and use short, descriptive subjects and clear sentences that are to the point.
- The use of internet abbreviations (Talk 2 U soon) and emoticons (☺) however, is not recommended.
- Do not write emails in all capitals as this may be interpreted as shouting and is generally considered unprofessional.
- Do not use cc: or bcc: fields unnecessarily or excessively.
- Ensure that everyone copied knows what action, if any, to take.

13. Revocation and change of access rights

13.1 Line Managers will let ICT Support know in advance of staff leavers or change of access rights for staff in advance wherever possible or within 24 hours' notice if not. This needs to include any external parties who have been granted access.

Document owner and approval

The Information Security Manager is the owner of this user agreement template and is responsible for ensuring that it is reviewed in line with the review requirements of the GDPR.

A current version of this document is available to all members of staff on the L.E.A.D. Academy Trust SharePoint and was published in June 2020.

This user agreement template was approved by the Chief Information Security Officer (CISO) on *[date]* and is issued on a version-controlled basis under his/her signature.

Signature: Date:

Change History Record

Issue	Description of Change	Approval	Date of Issue
1	Initial issue	Lee Jepson	16/04/2018
2	Updates	L.E.A.D. Academy Trust	June 2020

Appendix 4

Visitor and Volunteer Acceptable Use Agreement

For visitors and volunteers (and staff) who do not have access to school/setting ICT systems.

As a professional organisation with responsibility for children's safeguarding, it is important that all members of the community, including visitors and volunteers, are aware of their professional responsibilities when using technology. This AUA will help Rainbow Forge Academy ensure that all visitors and volunteers understand the Academy's expectations regarding safe and responsible technology use.

Policy scope

1. I understand that this AUP applies to my use of technology systems and services provided to me or accessed as part of my role within Rainbow Forge Primary Academy both professionally and personally. This may include use of laptops, mobile phones, tablets, digital cameras and email as well as IT networks, data and data storage and communication technologies.

2. I understand that Rainbow Forge Primary Academy AUA should be read and followed in line with the Academy staff Code of Conduct Policy.

3. I am aware that this AUA does not provide an exhaustive list; visitors and volunteers should ensure that all technology use is consistent with the Academy ethos, XXXXX Academy staff Code of Conduct and Safeguarding policies, national and local education and child protection guidance, and the law.

Data and image use

1. I will ensure that any access to personal data is kept in accordance with Data Protection legislation, including GDPR.

Classroom practice

1. I am aware of the expectations regarding safe use of technology in the classroom and other working spaces, including appropriate supervision of pupils, as outlined in the Academy Online Safety policy.

2. I will support teaching staff in reinforcing safe behaviour whenever technology is used on site and I will promote online safety with the children in my care.

3. I will immediately report any filtering breaches (such as access to illegal, inappropriate or harmful material) to the DSL in line with the Academy Safeguarding policy.

4. I will respect copyright and intellectual property rights; I will obtain appropriate permission to use content, and if videos, images, text or music is protected, I will not copy, share or distribute or use it.

Use of social media and mobile technology

1. I have read and understood the Academy Online Safety Policy which covers expectations regarding staff use of social media and mobile technology.

2. I will ensure that my online reputation and use of technology is compatible with my role within the Academy. This includes my use of email, text, social media, social networking, gaming and any other personal devices or websites.

3. I will take appropriate steps to protect myself online as outlined in the Online Safety policy.

4. I will not discuss or share data or information relating to pupils, staff, school/setting business or parents/carers on social media.

5. I will ensure that my use of technology and the internet will not undermine my role, interfere with my duties and will be in accordance with the Academy Online Safety policy and the law.

6. My electronic communications with pupils, parents/carers and other professionals will only take place within clear and explicit professional boundaries and will be transparent and open to scrutiny.
    a) All communication will take place via school-approved communication channels such as via a school-provided email address or telephone number and not via personal devices or communication channels such as via my personal email, social networking account or mobile phone number.
    b) Any pre-existing relationships or situations that may compromise this will be discussed with the DSL or Headteacher.

7. If I have any queries or questions regarding safe and professional practise online either in Rainbow Forge primary Academy or off site, I will raise them with the Designated Safeguarding Lead and the Headteacher.

8. I will not upload, download or access any materials which are illegal, such as child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act on my business or personal devices.

9. I will not attempt to access, create, transmit, display, publish or forward any material or content online that is inappropriate or likely to harass, cause offence, inconvenience or needless anxiety to any other person.

I will not engage in any online activities or behaviour that could compromise my professional responsibilities or bring the reputation of the Academy or the Trust into disrepute

Policy breaches or concerns

1. I will report and record concerns about the welfare, safety or behaviour of pupils or parents/carers to the Designated Safeguarding Lead in line with the Academy Online Safety and Safeguarding policies.

2. I will report concerns about the welfare, safety or behaviour of staff to the Headteacher, in line with the allegations against staff policy.

3. I understand that if the Academy believes that if unauthorised and/or inappropriate use, or unacceptable or inappropriate behaviour is taking place online, the Academy may invoke its disciplinary procedures.

4. I understand that if Rainbow Forge Primary Academy suspects criminal offences have occurred, the police will be informed.

I have read, understood and agreed to comply with Rainbow Forge Primary Academy visitor/volunteer Acceptable Use Agreement when using the internet and other associated technologies, both on and off site.

Name of visitor/volunteer: ……

Signed: …….....

Date (DDMMYY)……...

Appendix 5

Wi-Fi Acceptable Use Agreement

As a professional organisation with responsibility for children's safeguarding, it is important that all members of the Rainbow Forge Primary Academy community are fully aware of the boundaries and requirements when using the Academy Wi-Fi systems, and take all possible and necessary measures to protect data and information systems from infection, unauthorised access, damage, loss, abuse and theft.

This is not an exhaustive list and all members of the Rainbow Forge Primary Academy community are reminded that technology use should be consistent with our ethos, other appropriate policies and the law.

1. The Academy provides Wi-Fi for the Rainbow forge Primary Academy community and allows access for educational use only The password is held by the school office.

2. I am aware that the Academy will not be liable for any damages or claims of any kind arising from the use of the wireless service. The Academy takes no responsibility for the security, safety, theft, insurance and ownership of any device used within the Academy premises that is not the property of the Rainbow Forge primary Academy.

3. The use of technology falls under Rainbow Forge Primary Academy AUA, Online Safety, Code of Conduct and Safeguarding policies, which all pupils/staff/visitors and volunteers must agree to and comply with.

4. Academy-owned information systems, including Wi-Fi, must be used lawfully; I understand that the Computer Misuse Act 1990 makes the following criminal offences: to gain unauthorised access to computer material; to gain unauthorised access to computer material with intent to commit or facilitate commission of further offences or to modify computer material without authorisation.

5. I will take all practical steps necessary to make sure that any equipment connected to the Academy service is adequately secure, such as up-to-date anti-virus software and systems updates.

6. Use of the Academy wireless service is done at my own risk. By using this service, I acknowledge that security errors and hacking are an inherent risk associated with any wireless network. I confirm that I knowingly assume such risk.

7. The Academy accepts no responsibility for any software downloaded and/or installed, email opened, or sites accessed via the Academy wireless service's connection to the internet. Any damage done to equipment for any reason including, but not limited to, viruses, identity theft, spyware, plug-ins or other internet-borne programs is my sole responsibility; and I indemnify and hold harmless the Academy from any such damage.

8. The Academy accepts no responsibility regarding the ability of equipment, owned by me, to connect to the Academy wireless service.

9. I will respect system security; I will not disclose any password or security information that is given to me. To prevent unauthorised access, I will not leave any information system unattended without first logging out or locking my login as appropriate.

10. I will not attempt to bypass any of the Academy security and filtering systems or download any unauthorised software or applications.

11. My use of Rainbow Forge Primary Academy Wi-Fi will be safe and responsible and will always be in accordance with the Academy AUA and the law including copyright and intellectual property rights. This includes the use of email, text, social media, social networking, gaming, web publications and any other devices or websites.

12. I will not upload, download, access or forward any material which is illegal or inappropriate or may cause harm, distress or offence to any other person, or anything which could bring Rainbow Forge Primary Academy into disrepute.

13. I will report any online safety concerns, filtering breaches or receipt of inappropriate materials to the Designated Safeguarding Lead as soon as possible.

14. If I have any queries or questions regarding safe behaviour online, I will discuss them with Designated Safeguarding Lead or the Headteacher.

15. I understand that my use of Rainbow Forge Primary Academy Wi-Fi may be monitored and recorded to ensure policy compliance in accordance with privacy and data protection legislation. If the Academy suspects that unauthorised and/or inappropriate use or unacceptable or inappropriate behaviour may be taking place, then the Academy may terminate or restrict usage. If Rainbow Forge Primary Academy suspects that the system may be being used for criminal purposes, the matter will be brought to the attention of the relevant law enforcement organisation.

I have read, understood and agreed to comply with Rainbow Forge Primary Academy Wi-Fi acceptable Use Agreement.

Name ……..

Signed: ……Date (DDMMYY)……

Appendix 6

Remote Learning and Working Guidance

Remote learning, also often referred to as distance learning, is simply a method of learning which does not bring pupils into face-to-face contact with the teacher in a physical location. It means pupils can learn away from the classroom and often employs online methods such as webinars, e-learning, live-streaming or the ability to download resources and materials.

This guidance has been developed in line with the Academy's Safeguarding policy and the Online Safety policy. In using this guidance, the Academy community must follow these overarching policies as the basis for providing remote learning.

This remote learning guidance aims to:

- ensure consistency in the Academy approach to remote learning
- set out expectations for all members of the Academy community with regards to remote learning
- provide appropriate guidelines for data protection.

Staff

Staff should always discuss any general concerns or potential policy breaches with the DSL or a member of leadership staff as soon as possible.

Resources should be used in line with existing teaching and learning policies, taking licensing and copyright into account.

Staff should continue to follow professional behaviour expectations and maintain professional boundaries in relation to personal online behaviour expectations.

Staff should always use school-approved communication channels and not to use any personal accounts; where possible staff should use school provided devices. Using personal social media accounts or direct messengers with learners or parents/carers can undermine safeguarding policies and place learners and staff at risk of harm and allegations.

Staff are responsible for:

Setting work

If:

- A child is absent form school due to a medical reason but are able to complete school work and it has been agreed that they will learn remotely.
- The school closes due to a pandemic or another national emergency

When a child is learning remotely:

We aim to teach the same curriculum remotely as we do in school wherever possible and appropriate. However, we have needed to make some adaptations in some subjects. For example, PE will have learning set but this may differ slightly to the curriculum taught in school due to limitations of the children being at home.

The children will be sent a Zoom link to join the class for learning where this is possible.

The expectation is that the remote education (including remote teaching and independent work) will take pupils broadly the following number of hours each day:

Early Years	2 -3 hours of a variety of activities to complete with their parent
Key Stage 1	45 mins Maths 20 mins Reading 30 mins Phonics/spelling 30 mins English 1 hour of other subjects including History, Science, Geography, RE, Art, Music, PSHE & PE. 20 mins Story Time
Key Stage 2	1 hour Maths 30 mins Reading 15 mins Spelling/Grammar 45 mins English 1 hour of other subjects including History, Science, Geography, RE, Art, Music, PSHE, French & PE. 20 mins Story Time

- Remote learning will be set on Class Dojo each day.
- Zoom links, video links and worksheets will be uploaded each morning by 8.45am.
- Children will upload learning onto their Dojo portfolio.

We will use a variety of approaches:

- live teaching
- worksheets uploaded on Class Dojo
- recorded teaching, either by the teacher or using Oak National Academy lessons.
- printed paper packs produced by teachers (e.g. workbooks, worksheets)
- textbooks and reading books pupils have at home
- other websites supporting the teaching of specific subjects or areas, including video clips or sequences eg White Rose Maths.
- Doodle learning, Third Space Learning, and other online platforms.

Providing feedback on work

- Staff will check work on a daily basis and provide written feedback via Dojo.

Keeping in touch with pupils and parents:

- Staff will contact the parent daily via Dojo or phone during school hours. They will offer advice, support and encouragement.

Attending virtual meetings with staff, parents and pupils:

- Are expected to be dressed for meetings/live lessons (not in nightwear)
- Are expected to be in a quiet location with little background noise.

Subject Leads/Head of Department

Alongside their teaching responsibilities, as outlined above, subject leads are responsible for:

- Considering whether any aspects of the subject curriculum need to change to accommodate remote learning
- Monitoring the work set by teachers in their subject through regular meetings with teachers and reviewing work set
- Alerting teachers to resources they can use to teach their subject

Senior Leadership Team/Headteacher

Alongside any teaching responsibilities, senior leaders are responsible for:

- Coordinating the remote learning approach across the Academy
- Monitoring the effectiveness of remote learning through regular meetings with teachers and subject leaders, reviewing work set or reaching out for feedback from pupils and parents
- Monitoring the security of remote learning systems, including data protection and safeguarding considerations

Designated Safeguarding Lead

The DSL is responsible for:

- Ensuring the safety of vulnerable children by keeping in regular contact with parents/careers and the child were appropriate.
- Ensuring the child understands how to contact safe adults to share worries (Website button, Dojo, Childline)

IT staff/L.E.A.D. IT

Are responsible for:

- Fixing issues with systems used to set and collect work
- Helping staff and parents with any technical issues they're experiencing
- Reviewing the security of systems and flagging any data protection breaches to the data protection officer
- Assisting pupils and parents with accessing the internet or devices

Pupils and parents

Pupils are expected:

- Be contactable during the required times
- Complete work to the deadline set by teachers
- Seek help if they need it, from teachers or teaching assistants
- Alert teachers if they're not able to complete work

Parents are expected:

- Make the school aware if their child is sick or otherwise can't complete work

- Seek help from the school if they need it
- Be respectful when making any complaints or concerns known to staff

Data protection

Accessing personal data

When accessing personal data, all staff members will:

- Use information stored on Sharepoint
- Use school laptops, rather than their own personal devices

Sharing personal data

Staff members may need to collect and/or share personal data such as addresses, phone numbers, email addresses as part of the remote learning system. Such collection of personal data applies to our functions as a school and doesn't require explicit permissions.

While this may be necessary, staff are reminded to collect and/or share as little personal data as possible online.

Keeping devices secure

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- keeping the device password protected – strong passwords are at least eight characters, with a combination of upper and lowercase letters, numbers and special characters (e.g. asterisk or currency symbol)
- ensuring the hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device
- making sure the device locks if left inactive for a period
- not sharing the device among family or friends
- installing anti-virus and anti-spyware software
- keeping operating systems up to date – always install the latest updates.

Safety considerations

School

We do not expect pupils to sign up to anything with a personal email address. They will either be provided with a school email address or a username and password.

Parents:

- should ensure their child always keeps their login to this facility private and that they don't share their account with anyone
- remind children of their conduct online. As a member of the Academy community, they share a digital environment and their behaviour impacts the success of the online school community
- should assist their child on how to use the programmes to ensure they are safe. Careless use of programmes can lead to a breach of personal security, downloading viruses or malware or even contact from people they don't know
- remind their child to never accept instant messages, phone calls, screen sharing or files from someone they don't know.

Pupils

It is important to remember the same rules apply as being in the classroom, particularly in respect of behaviour and conduct. Focus on learning and don't get distracted by your surroundings. Treat remote learning the same as classroom learning by:

- using classroom language
- always conducting video learning in an open space at home
- only communicating through approved school portals and platforms
- sticking to teacher rules and guidelines around online learning
- not sharing passwords or other sensitive information
- not using school platforms to discuss personal matters
- remembering to be respectful and polite and avoid posting negative comments.

It is important that you send messages and any pictures or images required for class through approved school channels, such as internal learning portals or approved platforms. This will help to keep your personal information safe and secure.

Appendix 7

Guidance for use of Streaming Media Sites in Schools

Streaming Media Access

'Streaming' is the method for which media content, most commonly video and audio, is delivered to an end-user. The media is stored on one computer or server and, via the Internet, played back on another. Streaming media is not downloaded and stored on the receiving computer as a whole file, but is typically viewed on demand via a web page. YouTube and Vimeo are examples of popular streaming media websites.

L.E.A.D. Academy Trust recognises that teaching can be enriched by the use of streaming media in the classroom. However, there are many identified risks associated with this type of content.

This document is intended to highlight these risks and provide guidance on safe and responsible use of streaming media within the school. The document is not exhaustive and should be followed in line with other relevant policies put in place by the trust.

The Trust reserve the right to amend this policy at its discretion. In case of amendments, staff will be informed appropriately. This policy applies to all School Based employees and agents.

Context

There is a wide range of streaming media available via the internet and teachers are aware of the benefits of incorporating these resources into their teaching. However, due to the dynamic nature of the Internet, there are risks associated with this type of media where content is uploaded by the general population and is largely unregulated. This presents issues with the validity of the content, potential copyright and other legal issues, as well as its appropriateness for the intended audience.

Due to these risks, L.E.A.D. Academy Trust will allow access for teaching staff only and prevent students from accessing these types of sites.

Guidelines

As a member of staff using streaming media in the classroom you will be expected to adhere to the following guidelines:

Acceptable Use

The primary purpose for using streaming media is to enhance teaching and learning within the school. Streaming Media must only be used for legitimate teaching purposes, personal use is prohibited.

Media content should be viewed from start to finish and a full assessment made of its suitability for the intended audience. The content should be considered in the same way that you would consider any other resources used in your classroom.

Content must be assessed away from the view and earshot of students, preferably in a staff room or similar. Many classroom PC's are connected to interactive whiteboards and projectors, and may be configured for whole class display.

This must be considered when reviewing content.

Where a resource is deemed appropriate for use, it is recommended that it is downloaded and saved for future use. This will prevent any issues with online content being removed or changed. Separate tools are required to download streaming media to a PC, and examples are available on the Intranet.

If it is not possible to download the resource then the video should be viewed prior to each use, to ensure it remains suitable for the intended purpose.

Unacceptable Use

It is deemed inappropriate to view, create, access, download or publish material that is:

- Pornographic or Adult
- Racist, offensive, or derogatory
- Obscene
- Bullying
- Violent
- Fraudulent
- Likely to cause harassment to others
- Confidential
- Prejudicial to the school's or Council's best interests
- Not relevant to the business of the school or Council
- Likely to irritate or waste time of others
- Likely to breach copyright

Policy for use of Streaming Media Sites in Schools It is accepted that the teaching of certain subjects may present the need to use resources that could fall into one or more of the above categories. In such situations it is expected that the subject matter is presented in context; in a sensitive; balanced manner; and is appropriate for the age of the intended audience.

It is also expected that any home / school contracts regarding religion, sex education, parental wishes etc are considered when selecting media content.

Legal Risks

If you view, create, access, download or publish material that is pornographic, libellous, defamatory, offensive, racist or obscene, you, the school and L.E.A.D. Academy Trust can be held liable.

If you unlawfully view, create, access, download or publish confidential or personal information, you, the school and L.E.A.D. Academy Trust can be held liable.

If you unlawfully or without permission view, create, access, download or publish material that is copyrighted, you, the school and L.E.A.D. Academy Trust can be held liable for copyright infringement.

Appendix 8 – Guidance for Parents on the use of Vimeo

Dear Parent/Guardian,

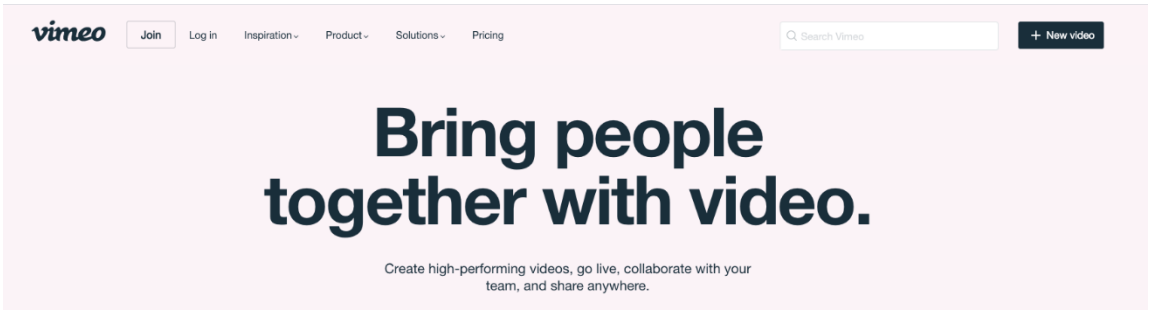
As we are increasing our use of online learning, we are using more systems and sites to help deliver and support this. Some of the platforms that we use to deliver videos for learning are not only used for education purposes but also for entertainment. This means that when pupils use the videos for learning they can also access wider areas of the sites.

Safeguarding pupils is very important to everyone at L.E.A.D. Academy Trust and we want to support parents to ensure that when their children are using these services, they are as safe as possible. One learning system that we use for maths videos and other subjects is VIMEO. This is the video hosting platform.

VIMEO has a wide variety of videos on its site, some of which may not be suitable for pupils to access. With this in mind we have put together a quick guide to help parents and carers put content filtering in place when using the software at home on the home internet connection. Please note that parents should always supervise and monitor their children when they are accessing the internet, even when content filtering is in place.

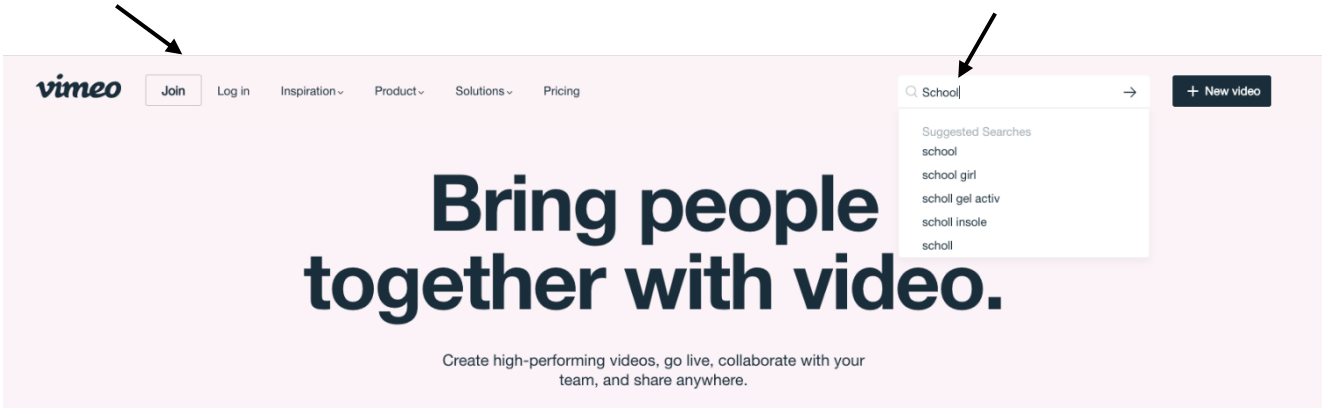
Step One:

Go onto VIMEO website – vimeo.com



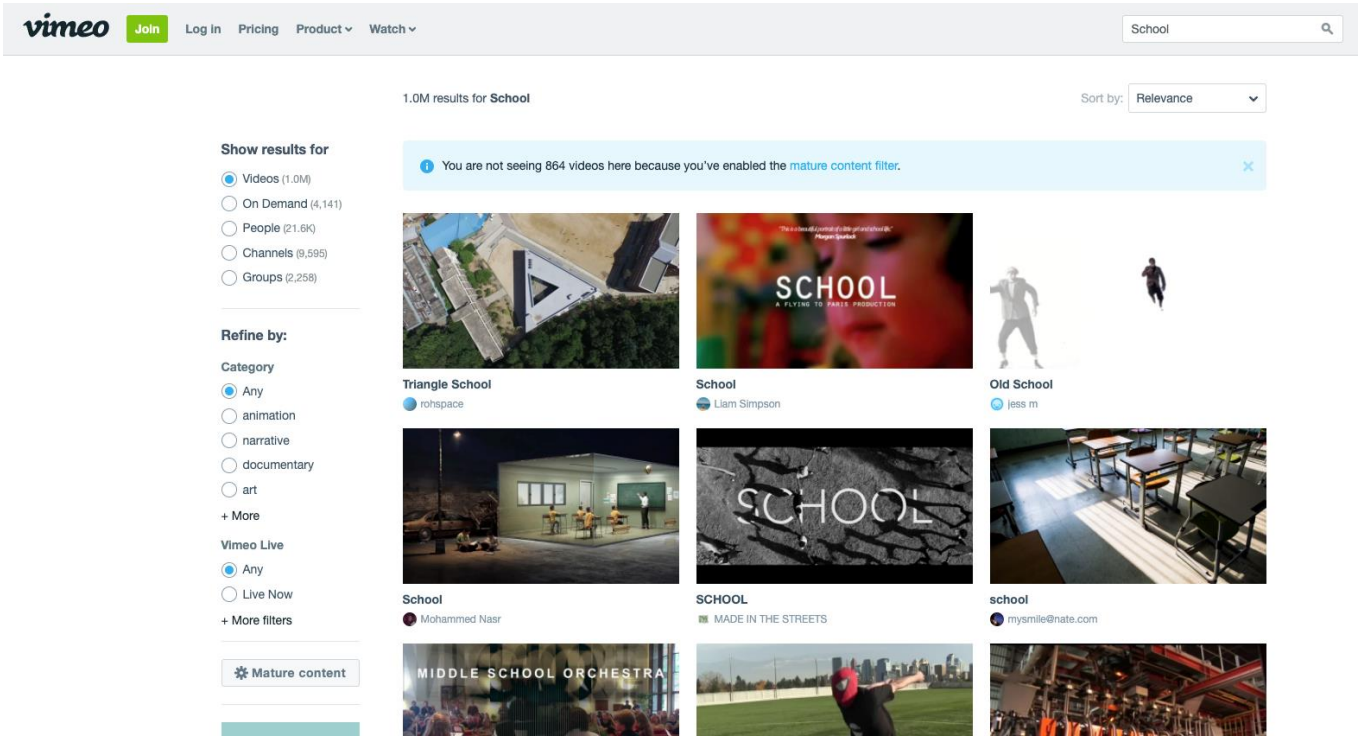
Step Two:

Type in 'School' in the search bar that's in the right-hand corner



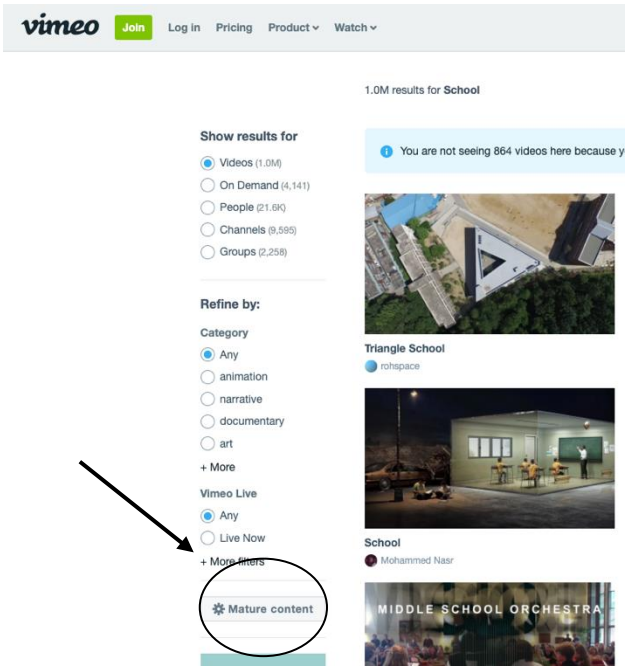
Step Three:

The page will then look like this –

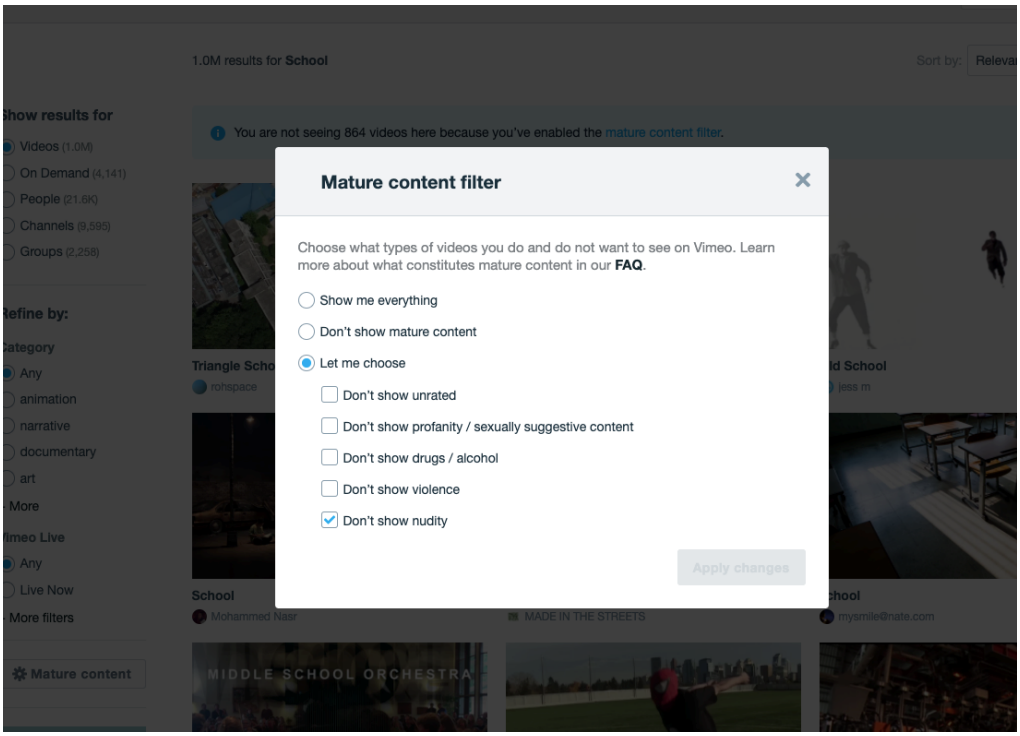


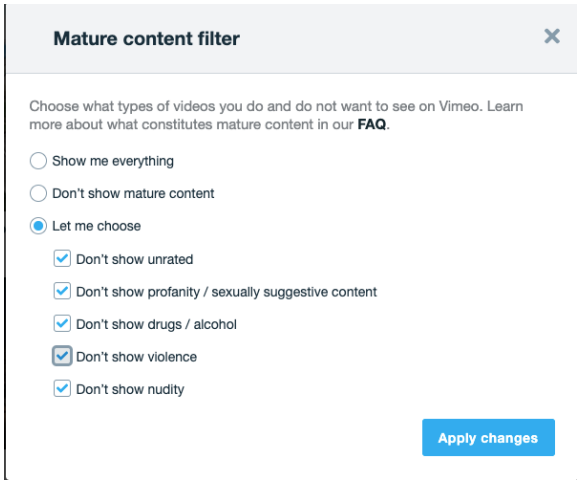
Step Four:

From there you will need to go 'Mature Content'



It will then give you the following settings:





Ensure the settings are ON under "Let me Choose" by ticking the appropriate boxes and 'Apply Changes'

I / we parents / carers of_____

Have: (please tick the relevant box)

a) Read and understood the guidance ☐

b) Would like further information from school ☐

Signed_____ Date_____

Appendix 9 - Social Media Support Tools – https://nationalonlinesafety.com/hub/resource

At National Online Safety we believe in empowering parents, carers and trusted adults with the information they need to hold an informed conversation about online safety with their children, should they feel it is needed. This guide focuses on one platform of many which we believe trusted adults should be aware of. Please visit www.nationalonlinesafety.com for further guides, hints and tips for adults.

Facebook is an online social media platform that has over 2 billion users across the globe. It was initially for university students but soon expanded out and since 2006, anyone over the age of 13 is able to join the platform. It is available on all devices from your desktop and laptop computer to smartphones and tablets. Users can add photos and videos, update their status, interact with others and catch up with the latest news. Despite requiring users to be over 13, there are no age verification measures and children can easily create an account. It's therefore important that parents familiarise themselves with the main features of the platform to ensure their young ones remain safe if and when they use it.

AGE RESTRICTION 13+ If under 18, supervision of a parent or legal guardian required.

What parents need to know about FACEBOOK

ADDICTIVE NATURE

Facebook can be hugely addictive as it offers a physiological high and a quick reward cycle which comes from the likes and comments on shared posts. Communication is so instant now that teenagers are always checking, and it can sometimes feel like self-worth. This keeps children going back, encouraging them to post things and also increases the Fear Of Missing Out (FOMO) that is commonplace today. On the flip side, because of the way teenagers interact these days through Facebook and Facebook Messenger, they can seem addicted even when they're not.

CYBERBULLYING

Around a quarter of children have experienced online abuse, according to Ofcoms 2019 'Online Nation' report. Figures show that 23% have been cyberbullied, 39% subjected to abusive language and a fifth have been trolled. On Facebook, teenagers can receive communication in a number of ways, from private messages in Messenger to public comments on profiles, pages and posts to pages or groups set up just to torment a victim. Exclusion from pages or groups to cause the victim to feel left out has also been seen.

FUTURE IMPACT

Regardless of age, anything that's posted on Facebook, or other social media platforms, develops a personal brand and leaves a digital footprint that is there forever. It can be difficult to explain the consequences but many universities (and employers) look at Facebook before making a decision on accepting people. It is therefore wise to always think twice before posting anything online you wouldn't want people to hear or see offline.

STRANGERS/FAKE PROFILES

Generally, people are who they say they are online. That said, much like the real world, Facebook isn't free of malicious users and children have received friend requests from people they don't know, including individuals who may look to take advantage of young and impressionable children.

OVERSHARING

Facebook encourages you to share "what's on your mind" but children need to be aware of what they're revealing about themselves online. Facebook allows users to share their location, create live videos and much more. Some photos can be traced using file data, too, so it's important to keep a tight group and share only with people you know.

INAPPROPRIATE ADS

While Facebook is getting ever stricter on the content of ads and who they are targeted to, there is still the chance that children could be subject to ads during their experience on the platform. This could be innocuous but is worth bearing in mind when using the app.

LIVE STREAMING

Facebook Live provides users with the ability to stream video live-time to their friends and followers or watch other people's broadcasts live. During the video, people can react and comment and it's difficult to moderate the content given everything happens in real-time. This could mean your child is exposed to inappropriate material or worse still, could be cajoled into doing something online by others which they wouldn't normally do.

PRIVATE MESSAGING

Facebook Messenger is closely linked to your Facebook profile and provides the ability to share private messages away from friends and family. It is therefore important that parents ask their children who they are communicating with and ensure that the only people they are exchanging messages with are people that they also know in real life.

National Online Safety® #WakeUpWednesday

Safety Tips For Parents

MAKE PROFILES PRIVATE

Within the settings of a Facebook account, you can choose whether a profile is public or private. Make sure that your child's setting is switched to private. This way they will only be able to interact with friends and people they know within the platform.

LEAD BY EXAMPLE

Show your children how and why you use Facebook. This will help to demonstrate that it can be used safely when used in an appropriate manner and help to reduce the risk of them encountering harmful content.

SHARE DEVICES

Depending on the age of your children, it's worth considering letting them use Facebook from a general family iPad or laptop. This allows them to use it without being constantly connected everywhere they go and may give you more reassurance around what they are doing on the app.

REPORT VIOLATIONS

On Facebook you're able to hide people or groups and report things that are harmful. Make sure you spend some time to show your children how this works and why it's important to do so before they start spending serious time on the platform.

RESPECT BOUNDARIES

As with anything, there are potential risks and dangers on Facebook but once you've talked about the ideas of safety on the platform, give children some space. Trust them to make smart choices but always be open to talking about social media.

CHECK-IN

Once they've had some time to use the platform, don't be afraid to check in and see if there's anything on Facebook they'd like to discuss. This isn't always easy but being open with your children is the best way to deal with any issues head on.

Meet our expert

Alex Wright is a former Facebook employee and social media expert with over 15 years' experience working in digital media. He has worked with some of the biggest organisations in the world and has a wealth of knowledge in understanding how social media platforms work and how they engage their audience.

SOURCES: http://facebook.com, https://www.independent.co.uk/life-style/social-media-addiction-young-children-under-five-youtube-instagram-a8953411.html, https://www.independent.co.uk/life-style/health-and-families/cyberbullying-social-media-children-online-abuse-facebook-research-ofcom-ico-a8936366.html, https://thriveglobal.com/stories/how-social-media-affects-our-ability-to-communicate/, https://www.care.com/c/en-gb/stories/4275/5-dangers-of-social-media-to-discuss-with-you/

National Online Safety®

#WakeUpWednesday

12 Social Media Online Safety Tips

FOR CHILDREN WITH NEW DEVICES

With Christmas only a few weeks away, many of you will be using social media to share your excitement with friends and family. Being active on social media is a great way to show others how much fun you're having, but it's important that you know how to use these apps safely and securely so that bad things don't happen. By following our safety tips below, you can make sure that your personal information stays private, your postings are positive and that your social media use overall is responsible, healthy and most of all enjoyable.

1 DON'T ACCEPT FRIEND REQUESTS FROM STRANGERS

Make sure that you set your profile to private so that people you don't know can't find you online. Always tell a trusted adult if a stranger or somebody you don't know sends you a message or a friend request.

2 NEVER SHARE YOUR PERSONAL INFORMATION WITH PEOPLE YOU DON'T KNOW

Keep your personal information personal. Sometime people online aren't always who they say they are and might ask you to share things that you don't feel comfortable sharing.

3 DON'T SHARE EMBARRASSING PHOTOS OR VIDEOS OF OTHERS ONLINE

This could really upset them and could get you into a lot of trouble. Always think twice before posting anything on social media and treat people online as you would in real-life.

4 NEVER SEND NAKED PICTURES OF YOURSELF TO OTHERS

This is illegal if you are under 18 and you could get into trouble with the Police. If you are being pressured by someone, always say no and tell a trusted adult. Even if you think it is innocent fun, the photo could be shared with other people and you won't be able to control who else sees it.

5 CREATE A POSITIVE ONLINE REPUTATION

Always be kind and polite when posting comments on social media and only upload pictures and videos of things you are proud of. This forms part of your digital footprint. Everything you do online can be tracked and monitored and could affect what people think of you in real-life if it is negative.

6 LIMIT YOUR SCREEN TIME

Social media can be addictive, and it is easy to keep checking newsfeeds or your notifications every 5 minutes which can affect your behaviour and stop you from doing other things. Remember to only use your phone at certain times of the day, turn notifications off at bedtime and go out and have as fun as much as possible. This will keep you fit and healthy and make you appreciate there's more to life than just what's on social media.

7 BLOCK ONLINE BULLIES

Sometimes people might say nasty things to you online or post offensive comments on your pictures or videos. If this happens, always tell a trusted adult who will help you block them from your profile and support you in taking further action.

8 REPORT INAPPROPRIATE CONTENT

If you see something on social media that you don't like, offends you or upsets you, you should always report it to a trusted adult. You should also report it to the social media app who will be able to remove the content if it is against their user policy and can block the person who posted it.

9 ONLY USE APPS WHICH YOU ARE OLD ENOUGH TO USE

Before downloading any new social media app, always check the age-rating. If you need help, ask your parent or carer to make sure that the app is safe for you to use and never download anything which you are too young for as it may contain content that isn't safe for you to see.

10 ALWAYS SECURE ALL YOUR SOCIAL MEDIA PROFILES WITH A PASSWORD

This will help to keep your private information safe and won't allow others to access your profiles without your permission. Make sure your passwords are memorable and personal to you but something which other people can't guess, and always share them with your parents just in case you forget them.

11 ASK PARENTS TO SET-UP 'PARENTAL CONTROLS' FOR SOCIAL MEDIA

When you download a social media app, you should always ask a trusted adult to help you set it up for the first time. This will help you control who sees what you post, who can contact you and make sure you are able to enjoy using the app safely and securely.

12 ALWAYS TALK TO YOUR TRUSTED ADULT IF SOCIAL MEDIA IS MAKING YOU UNHAPPY

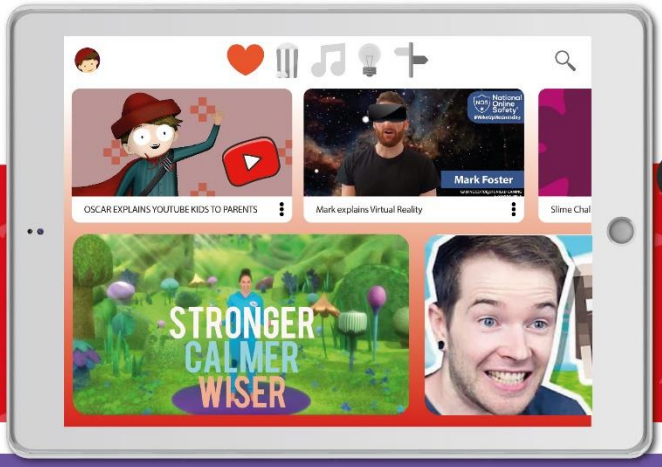
Sometimes, social media can make us feel bad about ourselves or sad that we aren't the same as someone else or doing the same things as someone else. Remember, if you ever feel this way, it's really important to talk to your trusted adult(s) like your parents, carers, other adult family members or a teacher, all of whom will be able to support you and discuss your feelings with you to help make you feel better.

At National Online Safety we believe in empowering parents, carers and trusted adults with the information they need to hold an informed conversation about online safety with their children, should they feel it is needed. This guide focuses on one platform of many which we believe trusted adults should be aware of. Please visit www.nationalonlinesafety.com for further guides, hints and tips for adults.

Although children of all ages often watch YouTube content directly via the website or main YouTube app, YouTube itself states that the only place children should be watching its videos is in the YouTube Kids app.

AGE RESTRICTION 4+

8 things parents need to know about YOUTUBE KIDS



1 SETTING UP

To set up the YouTube Kids app you need to do the following:

1 - Download the YouTube Kids app and connect your YouTube account.
2 - Specify your child's Name, Age and Birth Month.
3 - Select the types of videos to include in the app based on their age or select them yourself.
4 - If you choose to Approve Content yourself, you will be presented with some sample videos to accept or reject. You can select collections, shows, music or learning.
5 - Once chosen you are ready to use the app.

2 USING THE APP

Based on how you have set it up your child can then use the app to explore a safe set of videos. It's worth noting that YouTube Kids uses algorithms to ensure safe videos rather than a personal check, so it's possible for videos to slip through. If an inappropriate video does appear you can select the menu in the top right to block and report it. This not only helps your child but also improves the YouTube Kids app as a whole.

3 ADVERTISEMENTS

It's worth remembering that even in YouTube Kids, children will still see adverts. These are marked as "Ad" and preceded by an ad intro. The types of advertisements and products are checked to follow YouTube's advertising policies which exclude things like food and beverages. However, there can be toys or other items included in videos directly by creators themselves to advertise them. aYou can remove adverts in YouTube Kids, like the main YouTube, by subscribing to YouTube Premium. This also has the added benefit that you can download videos for offline viewing, you can also watch videos in the background while using other apps. This can be really useful if you have a long journey to take children on.

As with television adverts or bus stop posters, it's a good idea to talk to children about how adverts work and help them to recognise them. In my family, I remember pointing out the grinning children, added sound and light effects and exciting narration in TV ads. It's important to do this for other forms of advertising as well. It's important to understand how YouTube Kids collects information about your child's viewing and how this relates to advertising and video content. When they watch a video, the device, language, which videos they watch and searches they make are recorded. This is used to help suggest personalized content. It can also be used to serve contextual advertising, although the app does not allow interest-based advertising or remarketing.

4 SELECTING GREAT CONTENT

One of the best features on YouTube Kids is the ability to select channels, videos or collections of videos for your child to enjoy. This is a great opportunity to sit with your child and better understand what they want to watch. Are there particular topics or themes that resonate? Then you can check through different options in this area, and together with them choose the best matching channels.

The YouTube Kids app also enables you to disable the Search feature to avoid young children stumbling upon content designed for older viewers. The app also avoids videos from inappropriate channels being suggested to watch next. If you have selected content for your child only those will come up. If you have set an age limit, only videos deemed appropriate for that age will be suggested.

@CraftingWithAarav
@JaydenGaming
@AllaboutFrankie
@SuzeyPlays

5 VIEWING TIME

There are a number of ways you can administer how long a child can watch YouTube videos in a day. In the YouTube Kids app, you can set a timer before handing your child the smartphone or tablet. Once the time has run out the video will be paused.

You can also set limits on iPhones and iPads in the Screen Time section of the Settings. This not only enables you to see how long they play but specify how and when they can do this. You can apply similar limits on Android devices via the Family Link app settings. Other systems like the "Circle" system or features built into your Internet Router enable you to set limits across multiple devices which can be useful as children will often cruise to another smartphone, tablet or smart TV once their time has run out on their device.

As well as helping younger children not watch longer than is healthy, this is a good tool for discussion with older kids. Discuss together how long is appropriate to watch in a day and then agree on the limits. This ensures they see them as helpful rather than being policed.

6 RESTRICTIONS

As well as using the YouTube Kids app, you can also set up restrictions on other ways your family watches YouTube. Ensure you are logged in when using YouTube and turn on Restricted Mode in your User Profile. You can also set this at the bottom of the video page by clicking Restricted Mode: On. Ensure that you also click the Lock Restricted Mode on this browser to ensure so that other users can't turn it off.

7 WATCHING TOGETHER

Another good way to keep YouTube viewing positive is to spend time finding channels and content that your child will enjoy and benefit from. In my family, we each get together once a month and show each other our favourite videos from the last four weeks. This not only sparks conversations about what we've watched but enables us to share the things we've enjoyed watching.

8 RECOMMENDATIONS

For younger children, you can use the YouTube Kids app to keep tabs on what they have been watching. Tap on the Recommended icon on the top of the home screen and then swipe right. You will see videos with the play button on them and a red bar at the bottom. These are the videos your child has watched. Anywhere the bar at the bottom is mostly black is a video your child has skipped.

Meet our expert

Andy Robertson is a parent of three children and journalist who writes for national newspapers and broadcast television. His Taming Gaming book helps parents guide children to healthy play.

National Online Safety®
#WakeUpWednesday

www.nationalonlinesafety.com Twitter - @natonlinesafety Facebook - /NationalOnlineSafety