The Rainbow Multi Academy Trust
Building a Brighter Future...

TROON COMMUNITY PRIMARY SCHOOL
To be the best we can

Online Safety Policy

Guidance for staff regarding online safety
Good practice & guidelines

Policy Updated: September 2021

Policy Approved: ……………………………

Policy Review Date: September 2022

Taken from SWGfL
Education that Clicks

Online Safety Policy

Background / Rationale

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. Electronic communication helps teachers and *pupils* learn from each other. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. Children and young people should have an entitlement to safe internet access at all times.

The requirement to ensure that children and young people are able to use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound. A school online safety policy should help to ensure safe and appropriate use. The development and implementation of such a strategy should involve all the stakeholders in a child's education from the CEO, headteacher and governors to the senior leaders and classroom teachers, support staff, parents, members of the community and the pupils themselves.

The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote pupil achievement. However, the use of these new technologies can put young people at risk within and outside the school. Some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to / loss of / sharing of personal information
- The risk of being subject to grooming by those with whom they make contact on the internet.
- The sharing / distribution of personal images without an individual's consent or knowledge
- Inappropriate communication / contact with others, including strangers
- Online bullying
- Access to unsuitable video / internet games
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- The potential for excessive use which may impact on the social and emotional development and learning of the young person.

Many of these risks reflect situations in the off-line world and it is essential that this online safety policy is used in conjunction with other school policies (eg behaviour, anti-bullying and child protection policies).

As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build pupils' resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks.

The school must demonstrate that it has provided the necessary safeguards to help ensure that they have done everything that could reasonably be expected of them to manage and reduce these risks. The online safety policy that follows explains how we intend to do this, while also addressing wider educational issues in order to help young people (and their parents / carers) to be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.

The Rainbow Multi Academy Trust (Rainbow MAT) comprises five primary school in West Cornwall. Penponds School, St Meriadoc CE Infant Academy, St Meriadoc CE Junior Academy, St Ives Infant School and Troon School that have joined together to deliver high quality education for children 2-11 years of age. We believe in building a brighter future for our children and actively promote self-belief and a love of learning that will enable our children to achieve their full potential.

Development/Monitoring / Review of this Policy

This online safety policy has been developed by a working group made up of:

- CEO – Sam Jones
- School Online Safety Lead - Debi Ashworth
- Headteacher / Head of School - Sarah Wilkins
- Teachers
- Support Staff
- ICT Network Manager – Glyn Pascoe (iCT4 Ltd)
- Governors / Online Safety Governor - Lauren Collins

Consultation with the whole school community has taken place through the following:

- Staff meetings
- School eCadets / pupils
- INSET Day
- Governors meeting
- Parents evening
- School websites / newsletters

Schedule for Development / Monitoring / Review

This online safety policy was approved by the Governing Body:	September 2021
The implementation of this online safety policy will be monitored by the:	Online Safety Lead, Senior Leadership Team, Network manager & ICT technician
Monitoring will take place at regular intervals:	at least once a year
The Governing Body will receive a report on the implementation of the online safety policy generated by the monitoring group (which will include anonymous details of online safety incidents) at regular intervals:	at least once a year
The Online Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place. The next anticipated review date will be:	September 2022
Should serious online safety incidents take place, the following external persons / agencies should be informed:	Cornwall Council Child Protection Team, LADO, Police Commissioner's Office

The school will monitor the impact of the policy using:

- Logs of reported incidents
- Monitoring logs of internet activity (including sites visited) /filtering
- Internal monitoring data for network activity
- Surveys / questionnaires of
  - pupils (eg Ofsted "Tell-us" survey / CEOP ThinkUknow survey)
  - parents / carers
  - staff

Scope of the Policy

This policy applies to all members of Rainbow MAT community (including staff, pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of Rainbow MAT Schools ICT systems, both in and out of school.

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

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

Roles and Responsibilities

The following section outlines the roles and responsibilities for online safety of individuals and groups within the school:

Governors:

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about online safety incidents and monitoring reports. A member of the Governing Body has taken on the role of Online Safety Governor. The role of the Online Safety Governor will include:

- regular meetings with the Online Safety Co-ordinator
- regular monitoring of online safety incident logs
- regular monitoring of filtering / change control logs
- reporting to relevant Governors committee / meeting

Headteacher/Head of School and Senior Leaders:

- The CEO/Headteacher/Head of School has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day to day responsibility for online safety will be delegated to the Online Safety Co-ordinator or Senior Leaders as necessary.
- The CEO/Headteacher/Head of School and another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff. (see SWGfL flow chart on dealing with online safety incidents – included in a later section – "Responding to incidents of misuse" and relevant Local Authority HR / disciplinary procedures).
- The CEO/Headteacher/Head of School/Senior Leaders are responsible for ensuring that the Online Safety Coordinator and other relevant staff receive suitable CPD to enable them to carry out their online safety lead and to train other colleagues, as relevant.
- The CEO/Headteacher/Head of School/Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles. The network manager (iCT4 Ltd) will oversee the monitoring role within their SLA role.
- The Senior Leadership Team will receive regular monitoring reports from the Online Safety Lead.

Online Safety Lead:

- leads the Online Safety Group
- takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies / documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place

. ensures that staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.

- provides training and advice for staff
- liaises with the Network Manager and technical staff (iCT4Ltd)
- receives reports of online safety incidents and creates a log of incidents to inform future online safety developments.

- meets regularly with Online Safety Governor/Headteacher to discuss current issues, review incident logs and filtering / change control logs
- attends relevant meeting / committee of Governors
- reports regularly to Senior Leadership Team

Network Manager / Technical staff:

The Network Manager / IT Technician / Computing Co-ordinator is responsible for ensuring:

- that the school's ICT infrastructure is secure and is not open to misuse or malicious attack
- that the school meets required online safety technical requirements outlined in the SWGfL Security Policy and Acceptable Usage Policy and any relevant Local Authority Online Safety Policy and guidance
- that users may only access the school's networks through a properly enforced password protection policy, in which passwords are regularly changed.
- *the school's filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person*.
- that they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- that the use of the networks / internet / Virtual Learning Environment (VLE) / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Online Safety Co-ordinator (ICT Co-ordinator) / CEO / Headteacher / Head of School / Senior Leader / Class teacher for investigation / action / sanction
- that monitoring software / systems are implemented and updated as agreed in school policies

Teaching and Support Staff

Are responsible for ensuring that:

- they have an up to date awareness of online safety matters and of the current school Online Safety Policy and practices
- they have read, understood and signed the school Staff Acceptable Use Agreement
- they report any suspected misuse or problem to the Online Safety Lead / CEO / Headteacher / Head of School / Senior Leader / Class teacher for investigation / action / sanction
- all digital communications with pupils / parents / carers should be on a professional level and only carried out using official school systems
- online safety issues are embedded in all aspects of the curriculum and other school activities
- pupils understand and follow the Rainbow MAT Online Safety Policy and acceptable use policy
- pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities (where allowed) and implement current policies with regard to these devices in lessons, extra-curricular and extended school activities
- in lessons (in school and home online learning) where internet use is pre-planned pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches (how to use google safe search on www, use of Hector and completion of online safety incident log).

Designated Safeguarding Lead (Headteacher/Head of School)

Should be trained in Online Safety issues and be aware of the potential for serious child protection / safeguarding issues to arise from:

- sharing of personal data
- access to illegal / inappropriate materials

- inappropriate on-line contact with adults / strangers
- potential or actual incidents of grooming
- online-bullying

Online Safety Group

The Online Safety Group provides a consultative group that has wide representation from the school community, with responsibility for issues regarding online safety and the monitoring the Online Safety Policy including the impact of initiatives. The group will also be responsible for regular reporting to the Governing Body.

Members of the Online Safety Group (or other relevant group) will assist the Online Safety Coordinator with:

- the production / review / monitoring of the school Online Safety Policy.
- the production / review / monitoring of the school filtering policy and requests for filtering changes
- mapping and reviewing the online safety curricular provision – ensuring relevance, breadth and progression
- monitoring network / internet / incident logs
- consulting stakeholders – including parents / carers and the pupils about the online safety provision
- monitoring improvement actions identified through use of the 360-degree safe self-review tool

Pupils:

- are responsible for using the school digital technology systems in accordance with the Pupil Acceptable Use Agreement, which they will be expected to sign before being given access to school systems.
- eCadets/Digital Leaders (pupils from y3-6) will promote good online safety practice across the school and community.
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- will be expected to know and understand school policies on the use of mobile devices and digital cameras. They should also know and understand school policies on the taking / use of images and on online-bullying.
- should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that their school's Online Safety Policy covers their actions out of school, if related to their membership of a Rainbow MAT school.

Parents / Carers

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate safe way. The Rainbow MAT schools and Digital Leaders/eCadets will therefore take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website / Twitter / Facebook / VLE and information about national / local online safety campaigns / literature. Parents and carers will be encouraged to support their school in promoting good online safety practice and to follow the guidelines on the appropriate use of:

- endorsing (by signature) the Pupil Acceptable Use Agreement (AUA)
- digital and video images taken at school events

- accessing their school website / school Facebook page / school Twitter accounts / VLE / on-line pupil records

Community Users

Community Users who access Rainbow MAT schools systems / website / VLE as part of the wider School provision will be expected to sign a Community User Acceptable Use Agreement before being provided with access to school systems.

Policy Statements

Education – pupils

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

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

- A planned online safety programme should be provided as part of Computing / PSHE / other lessons and should be regularly revisited
- Key online safety messages should be reinforced as part of a planned programme of assemblies and pastoral activities
- Pupils should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Pupils should be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making.
- Rules for use of digital technologies / internet will be posted in all classrooms
- Pupils should be helped to understand the need for the pupil AUA and encouraged to adopt safe and responsible use both within and outside school
- Staff should act as good role models in their use of digital technologies, the internet and mobile devices
- In lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.

- It is accepted that from time to time, for good educational reasons, pupils may need to research topics (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (or other relevant designated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

Education – parents / carers

Many parents and carers have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's on-line experiences. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it.

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

- Letters home 'Thinkuknow', newsletters, magazine (Digital Parenting), website – online safety page, VLE
- Parents evenings and online safety briefings
- High profile events e.g. Safer Internet Day
- Reference to the relevant websites/publications for example: SWGFL "Golden Rules" for parents

Education – The Wider Community

The Rainbow Mat schools will provide opportunities for the community to gain from the school's online safety knowledge and experience. This may be offered through the following:

- Online safety messages targeted towards grandparents and other relatives as well as parents.
- Their school website, school Facebook and school Twitter accounts will provide online safety information for the wider community.
- Sharing their online safety expertise/good practice within the Rainbow MAT and other local schools.

Everyone has a role to play in empowering children to stay safe while they enjoy these new technologies, just as it is everyone's responsibility to keep children safe in the non-digital world.

Education & Training – Staff / Volunteers

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

- A planned programme of formal online safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out regularly.
- All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the school Online Safety Policy and Acceptable Use Agreements.
- The Online Safety Lead will receive regular updates through attendance at SWGfL / LA / other information / training sessions and by reviewing guidance documents released by SWGfL / LA and others.
- It is expected that some staff will identify online safety as a training need within the performance management process.
- This Online Safety Policy and its updates will be presented to and discussed by staff in staff / team meetings / INSET days.
- The Online Safety Lead / Network Manager will provide advice / guidance / training as required to individuals as required.

Training – Governors

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

- Attendance at training provided by the Local Authority / National Governors Association / SWGfL or other relevant organisation.
- Participation in school training / information sessions (assemblies) for staff or parents.

Technical – infrastructure / equipment, filtering and monitoring

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

- School technical systems will be managed in ways that ensure that the school meets the online safety technical requirements
- There will be regular reviews and audits of the safety and security of school technical systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to school technical systems. Details of the access rights available to groups of users will be recorded by the Network Manager (or other person) and will be reviewed, at least annually, by the Online Safety Committee.
- All pupils will be provided with a username and password by the Network Manager who will keep an up to date record of users and their usernames. KS1 will use class log-ons and passwords and be aware of the risks associated with shared access.

- The “administrator” passwords for the school technical system, used by the Network Manager must also be available to the CEO/Headteacher/Head of School or nominated senior leader and kept in a secure place.
- Users will be made responsible for the security of their username and password, must not allow other users 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 master/ administrator passwords for the school IT system used by the Network Manager must also be available to the Headteacher/Head of School and kept in a secure place (eg. school safe)
- Glyn Pascoe (iCT4Ltd), 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
- The school maintains and supports the managed filtering service provided by iCT4Ltd.
- Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored. There is a clear process in place to deal with requests for filtering changes. Filtering reports are emailed to the Online Safety coordinator and the Headteacher/Head of School when a user has attempted to access filtered websites or used key words and weekly blocked attempts and top blocked user reports.
- Internet filtering / monitoring should ensure that children are safe from terrorist and extremist material when accessing the internet.
- In the event of the Network Manager (or other person) needing to switch off the filtering for any reason, or for any user, this must be logged and carried out by a process that is agreed by the Headteacher / Head of School online safety coordinator.
- Any filtering issues should be reported immediately to the online safety committee or Network Manager who will report to SWGfL.
- Requests from staff for sites to be removed from the filtered list will be considered by the Network Manager and Headteacher. If the request is agreed, this action will be recorded and logs of such actions shall be reviewed regularly by the Online Safety Committee.
- School computing technical staff and ICT coordinator regularly monitor and record the activity of users on the school ICT systems and users are made aware of this in the Acceptable Use Policy. Rainbow MAT Schools use iCT4 Ltd for filtering and monitoring services to monitor activity.
- An appropriate system is in place (Online safety Incident Log Book) for users to report any actual / potential online safety incident to the Online Safety Coordinator and brought to the attention of the CEO/Headteacher/Head of School, if necessary. Completed logs are to be kept in a locked place at all times.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly.
- An agreed Acceptable Use Agreement for Guests is in place for the provision of temporary access of “guests” (eg trainee teachers, visitors) and Community Users (parents/carers /community users) onto the school systems. Staff are not to allow “guests” to use their login details.

- An agreed policy is in place regarding the downloading of executable files by users that the Network Manager is consulted before any installations are carried out to ensure that licences are upheld and security not breached.
- An agreed policy is in place regarding the extent of personal use that staff and their family members are allowed on laptops and other portable devices that may be used out of school. (see School Personal Data Policy)
- Installing programmes on school workstations / portable devices is not allowed unless agreed by the ICT coordinator, who will contact the Network Manager.
- An agreed policy is in place regarding the use of removable media (eg encrypted/password protected memory sticks / CDs / DVDs) by users on school workstations / portable devices. Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured. (see School Personal Data Policy)
- The school infrastructure and individual workstations are protected by up to date virus software.
- Staff and Chair of Governors are to use their own school issued email address for all work related communication.

Mobile Technologies

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

All users should understand that the primary purpose of the use mobile / personal devices in a school context is educational. The mobile technologies policy should be consistent with and inter-related to other relevant school polices including but not limited to the Safeguarding Policy, Behaviour Policy, Bullying Policy, Acceptable Use Policy, and policies around theft or malicious damage. Teaching about the safe and appropriate use of mobile technologies should be an integral part of the Rainbow MAT schools Online Safety education programme.

- The school Acceptable Use Agreements for staff, pupils/students and parents/carers will give consideration to the use of mobile technologies
- Rainbow MAT schools allow:

	School Devices		Personal Devices		
	School owned for single user	School owned for multiple users	Student owned	Staff owned	Visitor owned
Allowed in school	*Yes*	*Yes*	*Yes*[1]	*Yes*[1]	*Yes*[3]
Full network access	*Yes*	*Yes*			
Internet only					
No network access					

[1] Authorised device – purchased by the family. Permission given by the teacher for the device to be used in the class. Teacher to evaluate the educational content and value before it is shared with other pupils i.e. sharing Bloom's Project Homework challenges. Storage of student owned device will be in the teacher's desk so it will be only used at the appropriate time. The student owned device may not be given full access to the network as if it were owned by the school.

[2] Staff owned mobile devices will be allowed access to networks/internet if they are used for educational purposes and the meet the requirements of this policy:

- Filtering of the internet connection to these devices
- Data Protection
- Taking / storage / use of images
- The right to take, examine and search users devices in the case of misuse (England only) – n.b. this must also be included in the Behaviour Policy.

[3]The use of Guest mobile devices in school: may be allowed access to networks/internet if they are used for educational/training purposes and the meet the requirements of this policy:

- Complete a Guest Acceptable User Agreement
- Filtering of the internet connection to these devices
- Data Protection
- No taking / storage / use of images
- The right to take, examine and search users' devices in the case of misuse (England only) – n.b. this must also be included in the Behaviour Policy.

- Identification / labelling of personal devices
- Liability for loss/damage or malfunction following access to the network (likely to be a disclaimer about school responsibility).

Curriculum

Online safety should be a focus in all areas of the curriculum and staff and Digital Leaders/eCadets should reinforce online safety messages in the use of digital technology across the curriculum.

- in lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where pupils are allowed to freely search the internet, eg using safe search engines, staff should be vigilant in monitoring the content of the websites the pupils visit.
- It is accepted that from time to time, for good educational reasons, pupils may need to research topics (eg racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Network Manager (and other relevant person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.
- Pupils should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information

- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.

Use of digital and video images – Photographic, Video

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, staff, parents / carers and pupils need to be aware of the risks associated with sharing images and with posting digital images on the internet. Such images may provide avenues for online bullying to take place. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. There are many reported incidents of employers carrying out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular, they should recognise the risks attached to publishing their own images on the internet eg on social networking sites such as Facebook and Twitter.
- Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment. The personal equipment (not mobile phone cameras) of staff may only be used with permission of the Headteacher/Head of School under certain circumstances and the images are to be downloaded onto the school network and then deleted off the personal equipment.
- In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other *pupils* in the digital / video images.
- Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission.
- Photographs published on Rainbow MAT schools websites, newsletters, school and class Twitter accounts, class blogs or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images. Photographs and names of pupils will not be used on the school Facebook page.
- Pupils' full names will not be used anywhere online- school websites, school Facebook account, school Twitter accounts or class blogs, no pupil names will be used in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school websites/school social media/local press-see Parents / Carers Acceptable Use Agreement.
- Pupil's work can only be published with the permission of the pupil and parents or carers.

Data Protection

Personal data will be recorded, processed, transferred and made available according to the current data protection legislation.

The school must ensure that:

- It has a Data Protection Policy.
- It has paid the appropriate fee to the Information Commissioner's Office (ICO).
- It has appointed a Data Protection Officer (DPO)
- It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.
- Data held must be accurate and up to date. Inaccuracies are corrected without unnecessary delay.
- The lawful basis for processing personal data (including, where relevant, consent) has been identified and documented and details provided in a Privacy Notice. (see Privacy Notice section in the appendix)
- Where special category data is processed, a lawful basis and a separate condition for processing have been identified.
- Data Protection Impact Assessments (DPIA) are carried out.
- It has clear and understood arrangements for access to and the security, storage and transfer of personal data, including, where necessary, adequate contractual clauses or safeguards where personal data is passed to third parties e.g. cloud service providers.
- Procedures must be in place to deal with the individual rights of the data subject i.e. a Subject Access Requests to see all or a part of their personal data held by the data controller.
- There are clear and understood data retention policies and routines for the deletion and disposal of data.
- There is a policy for reporting, logging, managing and recovering from an information risk incident which recognises the requirement to report relevant data breaches to the ICO within 72 hours of the breach, where feasible.
- Consideration has been given to the protection of personal data when accessed using any remote access solutions.
- All schools / academies (n.b. including Academies, which were previously exempt) must have a Freedom of Information Policy which sets out how it will deal with FOI requests.
- All staff receive data handling awareness / data protection training and are made aware of their responsibilities.

Staff must ensure that they:

- At all times take care to ensure the safekeeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session or "locked" when idle within a session. Staff computers to be 'locked' when leaving the room, only to be unlocked with password.
- Transfer data using encryption and secure password school issued protected devices.

When personal data is stored on any school issued portable computer system, USB stick or any other removable media:

- the data must be encrypted and password protected
- the device must be password protected (many memory sticks / cards and other mobile devices cannot be password protected)
- the device must offer approved virus and malware checking software
- the data must be securely deleted from the device, in line with the Rainbow MAT policy (below) once it has been transferred or its use is complete

Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the Rainbow MAT currently considers the benefit of using these technologies for education outweighs their risks / disadvantages:

	Staff & other adults				Pupils			
Communication Technologies	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to school	✓							✓
Use of mobile phones in lessons – for explicit educational purposes		✓				✓		
Use of mobile phones in social time		✓						✓
Taking photos on school owned camera devices-NOT MOBILE PHONES	✓				✓			
Use of school owned mobile devices eg iPads	✓				✓			
Use of personal email addresses in school, or on school network only *after school clubs have finished*	✓							✓
Use of Rainbow MAT school email for personal emails - Use your professional judgement		✓						✓
Use of chat rooms /facilities-for educational purposes ONLY (VLE)		✓					✓	
Use of messaging APPS				✓				✓
Personal use of social media (such as Facebook)				✓				✓
Use of Rainbow MAT School Facebook page for information/communication purposes			✓					✓
Use of Rainbow MAT School Twitter Accounts for educational/information purposes			✓					✓
Use of Class Twitter Accounts for educational and information purposes TEACHER TO APPROVE TWEETS BEFORE TWEETED.		✓					✓	
Use of blogs-for educational purposes ONLY	✓					✓		

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

- The official Rainbow MAT school email service may be regarded as safe and secure and is monitored. Staff and pupils should therefore use only the school email service to communicate with others when in school, or on school systems (e.g. by remote access).
- Users need to be aware that email communications may be monitored
- Users must immediately report, to the Online Safety Lead – in accordance with the school policy, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.
- Any digital communication between staff and pupils or parents / carers (email, chat, VLE, Twitter etc) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or public chat / social networking programmes must not be used for these communications.
- Whole class or group email addresses will be used at KS1, while pupils at KS2 will be provided with individual school email addresses for educational use.
- Pupils should be taught about email safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material.
- Personal information should not be posted on school websites, school /class Twitter accounts or school Facebook pages and only official email addresses should be used to identify members of staff.

- Virtual meetings (Teams or Zoom) with pupils/parents will be recorded for safeguarding measures.

Social Media – Protecting Professional Identity

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

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

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

Rainbow MAT staff should ensure that

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

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

- *A process for approval by senior leaders – Head teacher/Head of School and will regularly check school and class twitter account*
- *Clear processes for the administration and monitoring of these accounts – involving at least two members of staff*
- *A code of behaviour for users of the accounts, including*
- *Systems for reporting and dealing with abuse and misuse*

- *Understanding of how incidents may be dealt with under school disciplinary procedures*

Personal Use:

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

Monitoring of Public Social Media

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

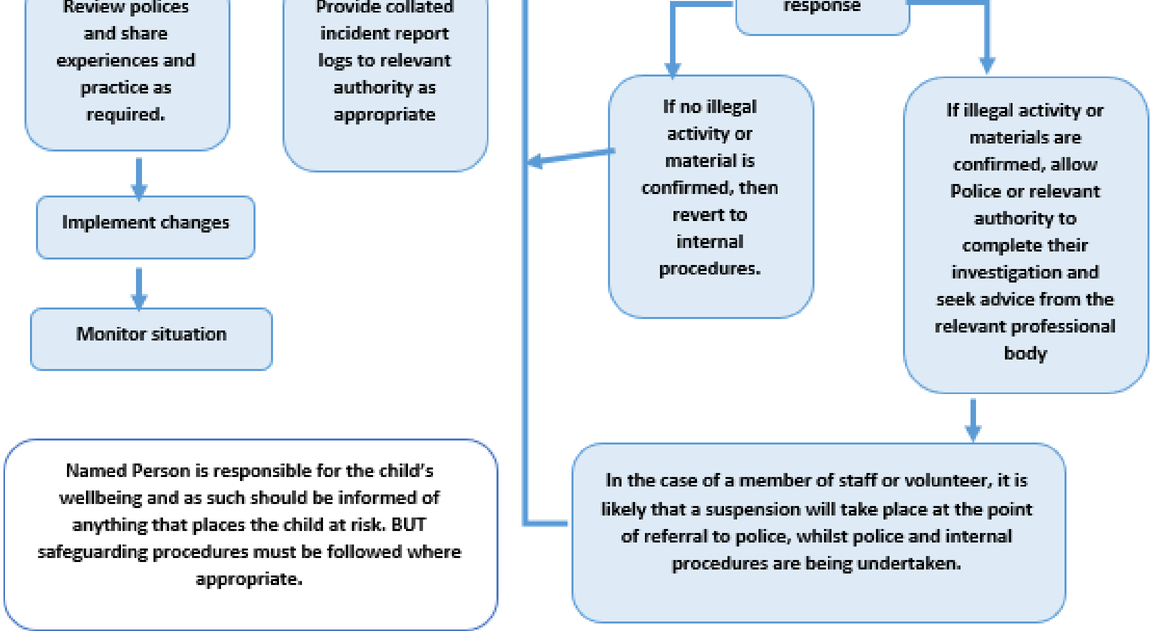
The *school's* use of social media for professional purposes will be checked regularly by the Headteacher/Head of School and *Online Safety Coordinator* senior risk officer to ensure compliance with the school policies.

Dealing with unsuitable / inappropriate activities

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

The Rainbow MAT believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in school or outside school when using school equipment or systems. The Rainbow MAT policy restricts certain internet 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, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978					✓
	promotion or conduct of illegal acts, eg under the child protection, obscenity, computer misuse and fraud legislation -Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					✓
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					✓
	criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986					✓
	pornography				✓	
	promotion of any kind of discrimination				✓	
	threatening behaviour, including promotion of physical violence or mental harm				✓	
	Promotion of extremism or terrorism				✓	
	any other information which may be offensive to colleagues/pupils or breaches the integrity of the ethos of the school or brings the school into disrepute				✓	
Using school systems to run a private business					✓	
Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school					✓	
Infringing copyright-uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions					✓	
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)					✓	
Creating or propagating computer viruses or other harmful files					✓	
Unfair usage-carrying out sustained or instantaneous high volume network traffic (downloading/uploading large files) that causes network congestion and hinders others in their use of the internet					✓	
On-line gaming (educational)			✓			
On-line gambling					✓	
On-line shopping /commerce for Teachers - outside teaching hours ONLY for personal use			✓			
File sharing - internal use for educational use			✓			
Use of social networking sites (such as Facebook) for personal use					✓	
Use of video broadcasting for educational purposes eg Teachertube NOTE: YouTube is unfiltered; Media needs to be fully audited before sharing with pupils.			✓			



Review polices and share experiences and practice as required.

Provide collated incident report logs to relevant authority as appropriate

response

Implement changes

Monitor situation

If no illegal activity or material is confirmed, then revert to internal procedures.

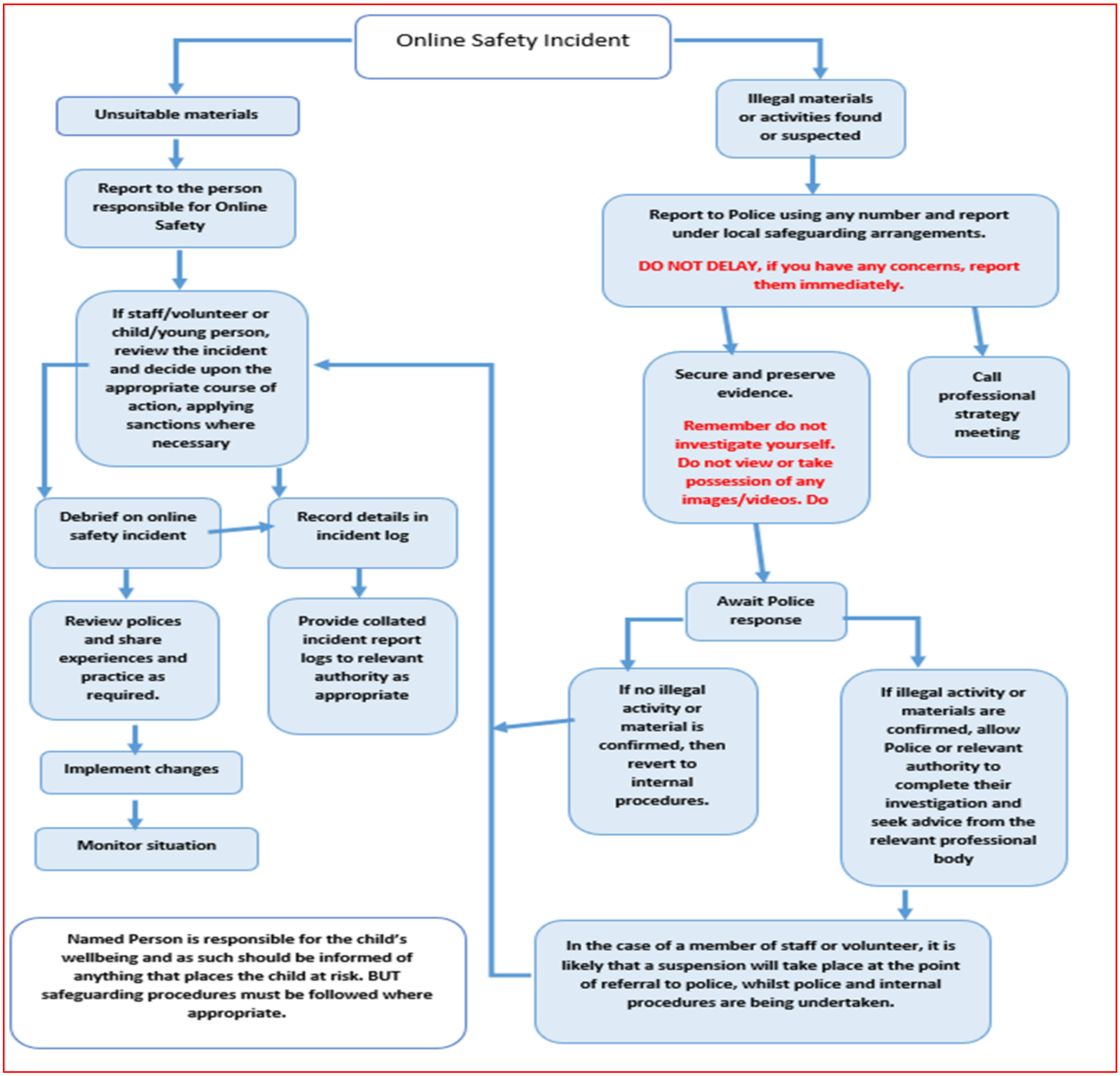
If illegal activity or materials are confirmed, allow Police or relevant authority to complete their investigation and seek advice from the relevant professional body

Named Person is responsible for the child's wellbeing and as such should be informed of anything that places the child at risk. BUT safeguarding procedures must be followed where appropriate.

In the case of a member of staff or volunteer, it is likely that a suspension will take place at the point of referral to police, whilst police and internal procedures are being undertaken.

f digital
nfringements of
iberate misuse.
misuse:

rt, in particular the



Online Safety Incident

Unsuitable materials

Report to the person responsible for Online Safety

If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary

Debrief on online safety incident

Record details in incident log

Review polices and share experiences and practice as required.

Provide collated incident report logs to relevant authority as appropriate

Implement changes

Monitor situation

Named Person is responsible for the child's wellbeing and as such should be informed of anything that places the child at risk. BUT safeguarding procedures must be followed where appropriate.

Illegal materials or activities found or suspected

Report to Police using any number and report under local safeguarding arrangements.

DO NOT DELAY, if you have any concerns, report them immediately.

Secure and preserve evidence.

Remember do not investigate yourself. Do not view or take possession of any images/videos. Do

Call professional strategy meeting

Await Police response

If no illegal activity or material is confirmed, then revert to internal procedures.

If illegal activity or materials are confirmed, allow Police or relevant authority to complete their investigation and seek advice from the relevant professional body

In the case of a member of staff or volunteer, it is likely that a suspension will take place at the point of referral to police, whilst police and internal procedures are being undertaken.

Other Incidents

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

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

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

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

School Actions and Sanctions

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

Actions / Sanctions

Pupils Incidents:	Refer to class teacher	Refer to CEO/ Headteacher/ Head of	CEO/ Headteacher/ Head of School to consider further	-Refer to Police	-Refer to technical support staff for action re filtering / security etc	-Inform parents / carers	-Removal of network / internet access rights	-Warning	-Further sanction eg detention / exclusion		
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).	✓	✓	✓								
Unauthorised use of non-educational sites during lessons	✓										
Unauthorised use of mobile phone / digital camera / other handheld device	✓	✓				✓					
Unauthorised use of social networking / instant messaging / personal email	✓	✓				✓					
Unauthorised downloading or uploading of files	✓	✓			✓	✓					
Allowing others to access school network by sharing username and passwords	✓	✓				✓					
Attempting to access or accessing the school network, using another student's / pupil's account	✓	✓				✓					
Attempting to access or accessing the school network, using the account of a member of staff	✓	✓				✓					
Corrupting or destroying the data of other users	✓	✓				✓	✓				
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature	✓	✓				✓					
Continued infringements of the above, following previous warnings or sanctions	✓	✓				✓					
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	✓	✓				✓					
Using proxy sites or other means to subvert the school's filtering system	✓	✓			✓	✓					
Accidentally accessing offensive or pornographic material and failing to report the incident	✓	✓			✓	✓					
Deliberately accessing or trying to access offensive or pornographic material	✓	✓	✓		✓						
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act	✓	✓	✓		✓	✓					

Actions / Sanctions

Staff Incidents:	Refer to Online safety Coordinator	Refer to Headteacher / Head of School	Refer to Governors	Headteacher / Head of School to consider further actions	-Refer to Local Authority / HR	-Refer to Technical Support Staff for action re filtering etc	-Refer to Police	-Warning	-Suspension	-Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).	✓	✓	✓	✓	✓	✓	✓			
Excessive or inappropriate personal use of the internet / social networking sites / instant messaging / personal email during school hours	✓	✓	✓	✓						
Unauthorised downloading or uploading of files	✓	✓	✓							
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account	✓	✓		✓		✓				
Careless use of personal data eg holding or transferring data in an insecure manner	✓	✓	✓	✓						
Deliberate actions to breach data protection or network security rules		✓	✓	✓						
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		✓	✓	✓						
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature		✓	✓	✓						
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils	✓	✓	✓	✓		✓				
Actions which could compromise the staff member's professional standing		✓	✓	✓						
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school. For example: Mentioning work related incidents on social networking sites.		✓	✓	✓						
Using proxy sites or other means to subvert the school's filtering system		✓	✓	✓						
Accidentally accessing offensive or pornographic material and failing to report the incident		✓	✓	✓						
Deliberately accessing or trying to access offensive or pornographic material		✓	✓		✓		✓			
Breaching copyright or licensing regulations	✓	✓	✓	✓		✓				
Continued infringements of the above, following previous warnings or sanctions		✓	✓	✓						

Acknowledgements

SWGfL would like to acknowledge a range of individuals and organisations whose policies, documents, advice and guidance have contributed to the development of this School Online safety Policy Template and of the 360 degree safe Online safety Self Review Tool:

- Members of the SWGfL Online Safety Group
- Avon and Somerset Police
- Representatives of SW Local Authorities
- Plymouth University Online Safety
- NEN / Regional Broadband Grids

Every effort has been made to ensure that the information included in this document is accurate, as at the date of publication in April 2018. However, SWGfL can not guarantee it's accuracy, nor can it accept liability in respect of the use of the material.

Appendices

Can be found on the following pages:

Online Safety
A School Charter for Action

Primary School

Rainbow Multi Academy Trust

We are working with staff, pupils and parents / carers to create a school community that values the use of new technologies in enhancing learning, encourages responsible use of digital technologies, and follows agreed policies to minimise potential online safety risks.

Our school community

Discusses, monitors and reviews our Online Safety policy on a regular basis. Good practice suggests the policy should be reviewed annually.

Supports staff in the use of digital technology as an essential tool for enhancing learning and in the embedding of online safety across the whole school curriculum.

Ensures that pupils are aware, through online safety education, of the potential online safety risks associated with the use of digital and mobile technologies, that all online safety concerns will be dealt with sensitively and effectively; that pupils feel able and safe to report incidents; and that pupils abide by the school's online safety policy.

Provides opportunities for parents/carers to receive online safety education and information, to enable them to support their children in developing good online safety behaviour. The school will report back to parents / carers regarding online safety concerns. Parents/carers in turn work with the school to uphold the online safety policy.

Seeks to learn from online safety good practice elsewhere and utilises the support of SWGfL and relevant organisations when appropriate.

Chair of Governors

Headteacher /
Head of School

eCadets /
Digital Leaders

Computing Acceptable Use Agreement for Pupils and Parents

The Rainbow MAT has installed computers, mobile devices and internet access to help our learning. These rules will keep everyone safe and help us be fair to others.

- ☺ I will access the system with my login and password, which I will keep secret.
- ☺ I will only use the digital devices for school work and homework unless I have permission for recreational use.
- ☺ I will not bring in software or personal devices into school without permission.
- ☺ I will ask permission from a member of staff before using the Internet.
- ☺ I will only e-mail people I know, or people that my teacher has approved. I will not open e-mails sent by someone I don’t know.
- ☺ I will ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have done something wrong
- ☺ The messages I send will be polite and responsible.
- ☺ I will never give out personal information about myself or others such as; full names, home addresses or telephone numbers, or arrange to meet anyone.
- ☺ I will report any unpleasant material or messages sent to me.
- ☺ I understand that the school may check my computer files and may monitor the Internet sites I visit.
- ☺ I will respect others’ work and property and will not access, copy, remove or otherwise alter any other user’s files, without the owner’s knowledge and permission.
- ☺ I know that if I break the rules I might not be allowed to use a laptop / tablet

I agree to follow the computing rules above.
Signed by child

____

I understand that my son’s / daughter’s activity on the school system will be monitored and that the school will contact me if they have concerns about possible breaches of the Acceptable Use Policy. I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child’s online safety.

Signed by parent/guardian

____ Date______________

The Rainbow Multi Academy Trust
Building a Brighter Future...

Dear Parents / Carers,

We are updating our Data Protection records, and would appreciate all parents/carers to once again give their permission for photographs and video clips to be used for school purposes on our school website, school/class Twitter and/or school publications or in the local press.

We would like to thank you for your continued support,

Miss D Ashworth   Mrs Wilkins
Online Safety Lead   Head of School

Conditions of use

This form is valid for the period of time your child attends this school. The consent will automatically expire after this time.

We will not re-use any photographs or recordings after your child leaves this school.

We will not use the personal details or full names (first name and surname) of any child in a photographic image or video on our website, school/class Facebook and Twitter Accounts, in our school prospectus or in any of our other printed publications.

If we use photographs of individual pupils, we will not use the name of that child in the accompanying text or photo caption.

If we name a pupil in the text, we will not use a photograph of that child to accompany the article.

We may include pictures of pupils and teachers that have been drawn by the pupils.

We may use group or class photographs or footage with very general labels, such as 'a science lesson' or 'making Christmas decorations'.

I agree that the Rainbow Multi Academy Trust can use images and video clips of my child in it's school publications, school/class Twitter/Facebook accounts and on the school website. I am happy for the press to take and use images of my child as part of school life with their first name only.   YES / NO

Name of child ……………………………………………………………………………………………………

Class ………………………………………………………………… Date ………………………………………

Signed………

Staff and Volunteer Acceptable Use Policy Agreement

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe access to the internet and digital technologies at all times.

This Acceptable Use Policy is intended to ensure:

- that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that staff are protected from potential risk in their use of technology in their everyday work.

The Rainbow MAT will try to ensure that staff and volunteers will have good access to digital technology to enhance their work, to enhance learning opportunities for students learning and will in return, expect staff and volunteers to agree to be responsible users

Acceptable Use Policy Agreement
I understand that I must use Rainbow MAT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users. I recognise the value of the use of digital technology for enhancing learning and will ensure that pupils receive opportunities to gain from the use of digital technology. I will, where possible, educate the young people in my care in the safe use of digital technology and embed online safety in my work with young people.
For my professional and personal safety:

- I understand that the *school* will monitor my use of the school digital technology and communications systems.
- I understand that the rules set out in this agreement also apply to use of these technologies (e.g. laptops, email, VLE etc.) out of school, and to the transfer of personal data (digital or paper based) out of school.
- I understand that the school digital technology systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.

I will be professional in my communications and actions when using school ICT systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital / video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (e.g. on the school website / VLE) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only use social networking sites in school in accordance with the Rainbow MAT's policies.
- I will only communicate with students / pupils and parents / carers using official school systems. Any such communication will be professional in tone and manner
- I will not engage in any on-line activity that may compromise my professional responsibilities.

The Rainbow MAT and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- When I use my mobile devices (laptops / tablets / mobile phones / USB devices etc) in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by the school about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- I will not use personal email addresses for school related correspondence.
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes).
- I will identify suspicious emails using the phishing flowchat and report suspicious phishing emails to the Online Safety Lead and/or the Network Manager.
- I will ensure that my data is regularly backed up, in accordance with relevant school policies.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless I have permission from the network manager.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the Rainbow MAT Staff Privacy Notice and Data Protection Policy. Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based Protected and Restricted data must be held in lockable storage.
- I understand that data protection policy requires that any staff or pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by MAT policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the internet in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of the school / Rainbow MAT:

- I understand that this Acceptable Use Policy applies not only to my work and use of school digital technology equipment in school, but also applies to my use of school systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the Rainbow MAT
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to CEO / Governors / Directors and / or the Local Authority and in the event of illegal activities the involvement of the police.

I have read and understand the above and agree to use the school digital technology systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Staff / Volunteer Name:………………………………………………………………………… Signed:………………………………………………………………………

Date:………………………………………………………

Phishing Flow Chart

The SWGfL Phishing Flowchart is here to help you analyse emails you're not sure about. Remember that it might not be right all the time!

Here's how to use it:

1. Start at the top left: "do you recognise the email address?" This is the actual address (e.g. infosec@swgflorg.uk), not just the 'display name' (e.g. "SWGfL Security Team).

2. "Is it from an organisation you know?" Here, you're looking at the email address to see if it's consistent with their website address (URL) and any emails they've sent you in the past.

3. "Does it have attachments and/or links?" If it does, these could be an attacker's way of trying to get something from you.

4. "Can you check the email address and attachments/links are legitimate?"
   - As in steps 1 and 2, look at the actual email address. It should match their genuine website (if you search through Google or another search engine).
   - Attachments can contain malware, so if you're not sure about the authenticity it's worth checking with your Glyn Pascoe (ICT4 Ltd) or the Online Safety Lead to see whether you can scan them for malware before opening.
   - You can hover your mouse over links to check where they will take you if clicked. This should be consistent with the sender's genuine website address.

5. "Can you contact the sender another way to verify it?" If you can speak to them in person, or over the phone (using a number you already have, or can find through their genuine website), that's the best way. You could also email them, but not by replying to the email they've sent you. Instead, create a new email and use the email address you already have, or one from their genuine website.

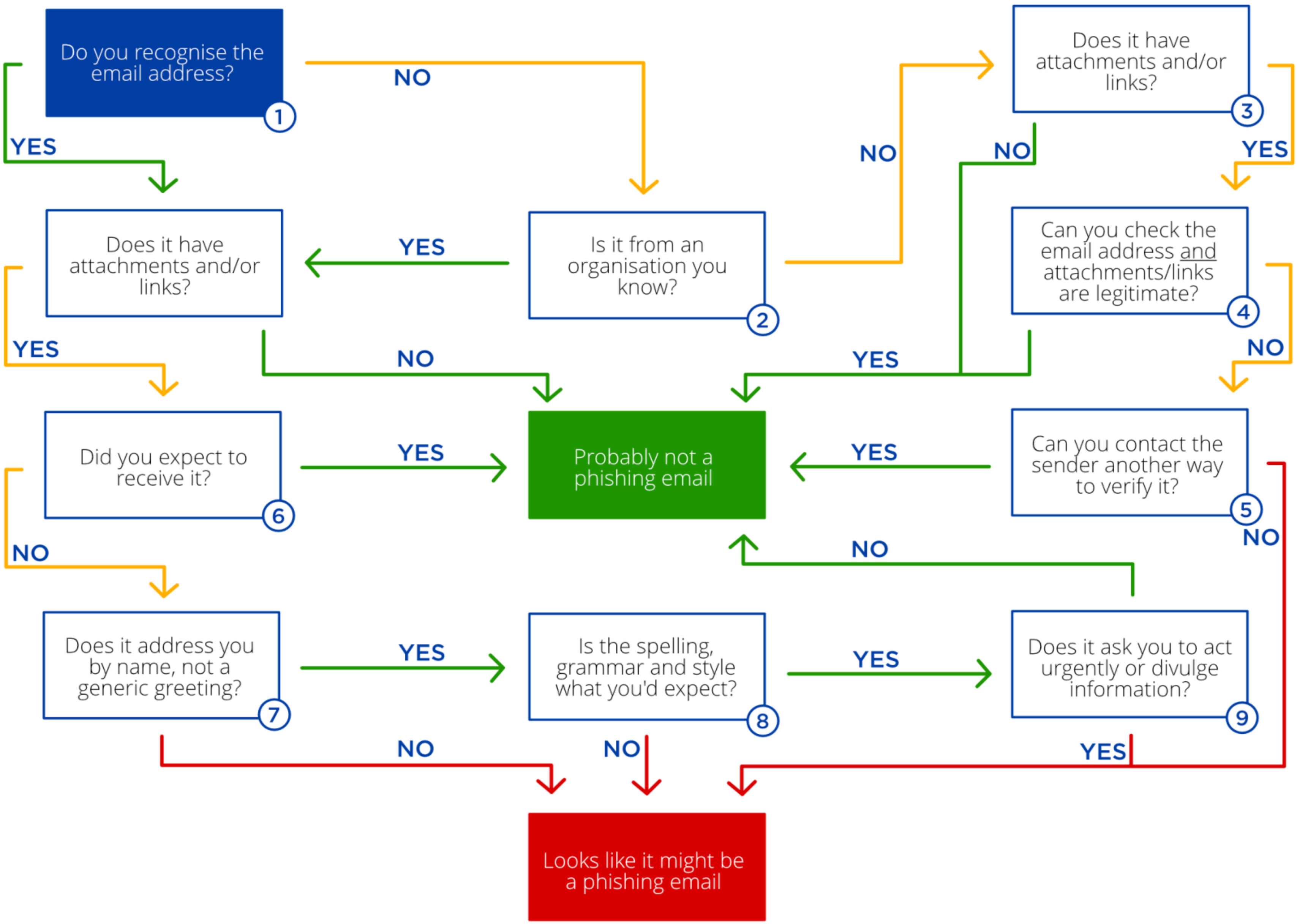
6. "Did you expect to receive it?" This is an important step: think carefully about how other people or organisations use email, and whether the email you're checking out fits in with this. If the timing or content don't fit, it's a warning sign. You could use the "can you contact the sender another way to verify it?" step here.

7. "Does it address you by name, not a generic greeting?" If some of the other criteria above are not checking out, and it's not addressed to you personally (particularly if it claims to be from a larger organisation whose technology should be able to address emails to you), it may well be phishing.

8. "Is the spelling, grammar and style what you'd expect?" Following on, if there are spelling or grammar mistakes, and/or a peculiar style, alongside other warning signs, that suggests it might be phishing.

9. "Does it ask you to act urgently or divulge information?" Equally, alongside other warning signs, adding time pressure or asking you to provide information is a classic sign of phishing.

SWGfL
Safe, Secure, Online



1 Do you recognise the email address?

2 Is it from an organisation you know?

3 Does it have attachments and/or links?

4 Can you check the email address and attachments/links are legitimate?

5 Can you contact the sender another way to verify it?

6 Did you expect to receive it?

7 Does it address you by name, not a generic greeting?

8 Is the spelling, grammar and style what you'd expect?

9 Does it ask you to act urgently or divulge information?

Probably not a phishing email

Looks like it might be a phishing email

iPad Acceptable Use Policy

User Responsibilities

- The iPad screen is made of glass and is therefore subject to cracking and breaking if misused; never drop or place heavy objects (book, laptops etc) on top of the iPad.
- Users must use protective cases/covers for their iPad.
- Only a soft cloth or approved laptop screen cleaning solution is to be used to clean the iPad screen.
- Do not subject the iPad to extremes of temperature.
- Do not store or leave unattended in vehicles.

Safeguarding and Maintaining as an Academic Tool

- Users may not photograph any other person without that person's consent
- Photographs of children must be in line with Consent Letter Agreement
- The whereabouts of the iPad should be known at all times.
- It is a user's responsibility to keep their iPad as safe and secure as possible.

Prohibited Uses

- Images of other people may only be made with the permission of the person, or parents of the person, in the photograph.
- The iPad should always be available in school to enhance classroom practice. It is not for personal use of social networking sites.

Lost, Damaged or Stolen iPad

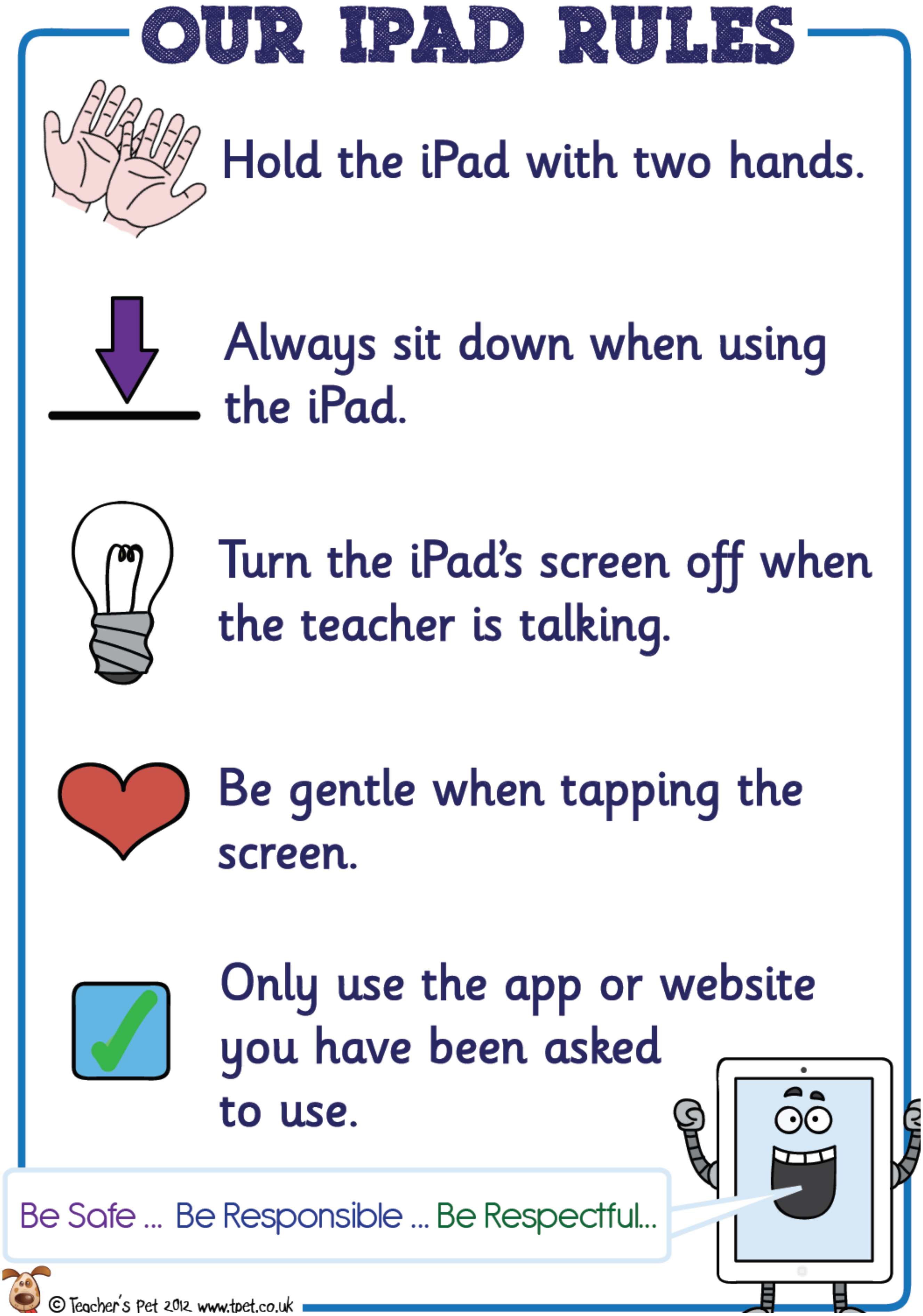
- If the iPad is lost, stolen or damaged, the IT Subject Leader or Headteacher/Head of School must be informed immediately.

Please read and sign below:
I have read, understand and agree to abide by the terms of the iPad Acceptable Use Policy.

Name:

Signature:

Date:



OUR IPAD RULES

Hold the iPad with two hands.

Always sit down when using the iPad.

Turn the iPad's screen off when the teacher is talking.

Be gentle when tapping the screen.

Only use the app or website you have been asked to use.

Be Safe ... Be Responsible ... Be Respectful...

Community Users / Guest Acceptable Use Agreement

For use by any Community User or Guest using our computing devices in the school for a short period of time. Rainbow MAT schools have installed computers, iPads and Internet access to help our pupils learning.

This Acceptable Use Agreement is intended to ensure:

- that community users of school digital technologies will be responsible users and stay safe while using these systems and devices
- that school systems, devices and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that users are protected from potential risk in their use of these systems and devices
- I will take responsibility for my own use of any technologies, making sure that I use them safely, responsibly and legally.

Acceptable Use Agreement

I understand that I must use the school systems and devices in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems, devices and other users. This agreement will also apply to any personal devices that I bring into the school:

- I understand that my use of school systems and devices and digital communications will be monitored
- I will not use a personal device that I have brought into school for any activity that would be inappropriate in a school setting.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.
- I will not access, copy, remove or otherwise alter any other user's files, without permission.
- I will ensure that if I take and / or publish images of others I will only do so with their permission. I will not use my personal equipment to record these images, without permission. If images are published it will not be possible to identify by name, or other personal information, those who are featured.
- I will not publish or share any information I have obtained whilst in the school on any personal website, social networking site or through any other means, unless I have permission from the school.
- I will not, without permission, make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a school device, nor will I try to alter computer settings, unless I have permission to do so.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).
- I understand that if I fail to comply with this Acceptable Use Agreement, the school has the right to remove my access to school systems.

As the school is collecting personal data by issuing this form, it should inform community users about:

The CEO, Headteacher/Head of School, Online Safety Lead and the Network Manager will have access to this form.
This form will be stored in the ICT AUP guest/supply/community user file in a locked cupboard in the office
This form will be kept for seven years
This form will be securely stored until its removed by Security Shredding Cornwall

I have read and agree to follow this code of conduct and to support the safe use of information communication technology throughout the school.

User Signature ______________________________________ Date_______ ___________

Full Name ____ (PRINT)

Position/Role ______________________________

The Rainbow Multi Academy Trust
Building a Brighter Future...

Dear Parents / Carers,
Our school is using Seesaw this year to build digital online portfolios. Seesaw gives your child creative tools to capture and reflect on their learning - in real time. Your child will add things like photos, videos, text, links, drawings and voice recordings to their Seesaw journal. Then this work is shared with you. Seesaw will give you a window into your child's learning process. Our students are excited to use this new tool in partnership with the great things our teachers do in their classrooms.

We need your help with Seesaw to ensure success at our School. You can download Seesaw's Parent App for iOS, Android, or use the web to view your student's learning. When your child adds new work, you will receive a notification to see, hear and respond to your child's learning item. You only have access to your own child's work and all of the content is stored securely. Seesaw journals are private and only accessible by the teacher, students, and parents.

In order for your child to use Seesaw, we need your permission. Because of the nature of the service, Seesaw does collect personally identifiable information, like your child's name, and photos, videos or voice recordings made by your child. Seesaw has a robust privacy policy https://web.seesaw.me/privacy and has committed to never share your child's personal information or journal content.

I hope that your child will enjoy using Seesaw to document and share their learning this year. You can learn more about Seesaw by visiting https://web.seesaw.me/ or contact your child's teacher with any questions about Seesaw.

With your help, we can continue building our school community of lifelong learners.

Headteacher/Head of School

- -

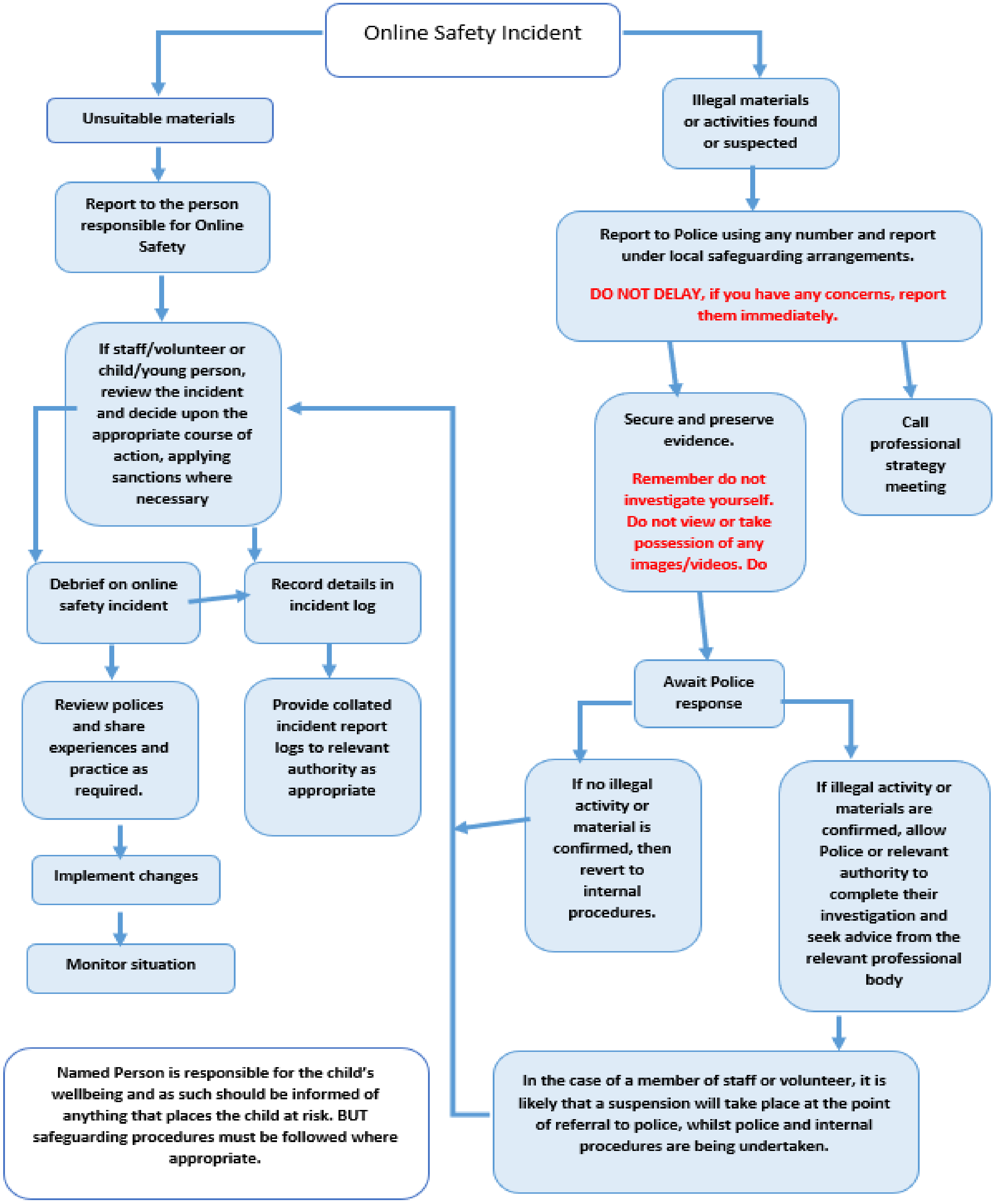
Please sign below and return the form.
I give consent for my child, listed below, to use Seesaw for class activities.

Child's Name: ____

Parent Printed Name: ____

Parent Signature: ____ Date: _________

Responding to incidents of misuse – flow chart



Online Safety Incident

Unsuitable materials

Report to the person responsible for Online Safety

If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary

Debrief on online safety incident

Record details in incident log

Review polices and share experiences and practice as required.

Provide collated incident report logs to relevant authority as appropriate

Implement changes

Monitor situation

Illegal materials or activities found or suspected

Report to Police using any number and report under local safeguarding arrangements.

DO NOT DELAY, if you have any concerns, report them immediately.

Secure and preserve evidence.

Remember do not investigate yourself. Do not view or take possession of any images/videos. Do

Call professional strategy meeting

Await Police response

If no illegal activity or material is confirmed, then revert to internal procedures.

If illegal activity or materials are confirmed, allow Police or relevant authority to complete their investigation and seek advice from the relevant professional body

In the case of a member of staff or volunteer, it is likely that a suspension will take place at the point of referral to police, whilst police and internal procedures are being undertaken.

Named Person is responsible for the child's wellbeing and as such should be informed of anything that places the child at risk. BUT safeguarding procedures must be followed where appropriate.

Online Safety Incident Log

All online safety incidents must be recorded by the Online Safety Lead or Headteacher/Head of School. This incident log will be monitored and reviewed regularly by the CEO, Headteacher/Head of School and Chair of Governors. Any incidents involving Online Bullying should also be recorded on the Integrated Bullying and Harassment Incident Form.

Date	Time	Type of Incident	Name of pupil/s and staff involved	System Details	Incident details	Resulting actions taken and by whom	Signature
01 Jan 2019 9.50am		Accessing Inappropriate Website	A.N Other – pupil AN Staff class teacher	Class1 Computer 1.5	Pupil observed by Class Teacher deliberately attempting to access adult websites	Pupil referred to Headteacher/Head of School and given warning in line with 1st time infringement of AUP. Site reported to SWGFL as inappropriate	

Only ONE incident per Online Safety Incident Log page. Please hand immediately to Online Safety Coordinator or Headteacher/Head of School. This completed log is to be kept in a locked place.

Record of reviewing devices/internet sites (responding to incidents of misuse)

Group	
Date	
Reason for investigation	

Details of first reviewing person

Name	
Position	
Signature	

Details of second reviewing person

Name	
Position	
Signature	

Name and location of computer/mobile device used for review (for web sites)

Web site(s) address/device	Reason for concern

Conclusion and Action proposed or taken

Training Needs Audit

Training Needs Audit Log

Group ……………………………………………………

Name	Relevant training in last 12 months	Identified training need	To be met by:	Cost	Review date

The Rainbow Multi Academy Trust
Building a Brighter Future...

Technical Security Policy
(including filtering and passwords)

Policy Updated: July 2021

Policy Approved: ……………………………………………

Policy Review Date: July 2022

Introduction

Effective technical security depends not only on technical measures, but also on appropriate policies and procedures and on good user education and training. The school will be responsible for ensuring that the *school infrastructure / network* is as safe and secure as is reasonably possible and that:

- users 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 school's policies).
- access to personal data is securely controlled in line with the school's personal data policy
- logs are maintained of access by users and of their actions while users of the system
- there is effective guidance and training for users
- there are regular reviews and audits of the safety and security of school computer systems
- there is oversight from senior leaders and these have impact on policy and practice.

Responsibilities

The management of technical security will be the responsibility of the network manager Glyn Pascoe (iCT4 Ltd).

Technical Security

Policy statements

The Rainbow MAT will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people receive guidance and training and will be effective in carrying out their responsibilities:

- School technical systems will be managed in ways that ensure that the school meets recommended technical requirements.
- There will be regular reviews and audits of the safety and security of school technical systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- Appropriate security measures are in place to protect the servers, firewalls, switches, routers, wireless systems, work stations, mobile devices etc. from accidental or malicious attempts which might threaten the security of the school systems and data.
- Responsibilities for the management of technical security are clearly assigned to appropriate and well trained staff (iCT4 Ltd).
- All users will have clearly defined access rights to school technical systems.
- Users will be made responsible for the security of their username and password must not allow other users 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 (Glyn Pascoe, iCT4 Ltd) 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.
- School technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement.
- Remote management tools are used by staff to control workstations and view users activity

- An appropriate system is in place (incident log book and email alerts from FastVue Reporter) for users to report any actual / potential technical incident to the Online Safety Lead / Network Manager / Headteacher / Head of School / School Secretary.
- An agreed policy is in place (Online Safety Policy is available and Community User/Guest AUP to be signed for the provision of temporary access of "guests" (e.g. trainee teachers, supply teachers, visitors) onto the school system.
- An agreed policy is in place (Rainbow MAT Staff data Privacy Notice and Data Protection Policy) regarding the use of removable media (eg memory sticks / CDs / DVDs) by users on school devices.
- The school 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 school site unless safely encrypted or otherwise secured. (see Rainbow MAT Staff data Privacy Notice and Data Protection Policy)

Password Security

A safe and secure username / password system is essential if the above is to be established and will apply to all school technical systems, including networks, devices, email and learning platforms..
An active two-factor authentication is required for staff to access the school network remotely (through their school emails accounts to MS SharePoint). All staff laptops are encrypted and have a two-factor authentication login.

Policy Statements

- All users will have clearly defined access rights to school technical systems and devices. Details of the access rights available to groups of users will be recorded by the Network Manager (or other person) and will be reviewed, at least annually, by the Online Safety Group (or other group).
- All school networks and systems will be protected by secure passwords that are regularly changed
- The "master / administrator" passwords for the school systems, used by the technical staff must also be available to the *Headteacher/Head of School* and kept in a secure place eg school safe. Consideration should also be given to using two factor authentication for such accounts.
- All users (adults and children) will have responsibility for the security of their username and password must not allow other users 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.
- Passwords for new users and replacement passwords for existing users will be allocated by Online Safety Lead and the Network Manager.
- Teachers will change their school network passwords at regular intervals.
- Teachers can generate usernames and passwords for online learning accounts such as Accelerated Reader and Oxford Owl Reading.
- Pupils will be taught the importance of password security

Staff Passwords

- All staff users will be provided with a username and password by Glyn Pascoe who will keep an up to date record of users and their usernames.

- the password should be a minimum of 8 characters long and must include three of – uppercase character, lowercase character, number, special characters
- *must not include proper names or any other personal information about the user that might be known by others*
- *the account should be "locked out" following six successive incorrect log-on attempts*
- *temporary passwords e.g. used with new user accounts or when users have forgotten their passwords, shall be enforced to change immediately upon the next account log-on*
- *passwords shall 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 school*
- should be changed at least every 60 to 90 days.
- should not re-used for 6 months and be significantly different from previous passwords created by the same user. *The last four passwords cannot be re-used.*

Training / Awareness

Members of staff will be made aware of the school's password policy:

- at induction
- through the school's online safety policy and password security policy
- through the Acceptable Use Agreement

Pupils will be made aware of the school's password policy:

- in lessons with discussions about how and why it's important to keep usernames and passwords secure
- through the Acceptable Use Agreement

Learner Passwords

- Records of learner usernames and passwords for foundation phase students/pupils can be kept in an electronic or paper-based form, but they must be securely kept when not required by the user. *Password complexity in foundation phase should be reduced (for example 6-character maximum) and should not include special characters. Where external systems have different password requirements the use of random words or sentences should be encouraged.*
- Password requirements for students/pupils at Key Stage 2 and above should increase as students' progress through school.
- Users will be required to change their password if it is compromised.
- Students will be taught the importance of password security, this should include how passwords are compromised, and why these password rules are important.

Audit / Monitoring / Reporting / Review

The responsible persons Glyn Pascoe, iCT4 Ltd and Online Safety Lead will ensure that full records are kept of:

- User Ids and requests for password changes
- *User logons*
- *Security incidents related to this policy*

Filtering

Introduction

The filtering of internet content provides an important means of preventing users from accessing material that is illegal or is inappropriate in an educational context. 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. It is important, therefore, to understand that filtering is only one element in a larger strategy for online safety and acceptable use. It is important that the school has a filtering policy to manage the associated risks and to provide preventative measures which are relevant to the situation in this school.

Responsibilities

The responsibility for the management of the school's filtering policy will be held by Glyn Pascoe, iCt4 Ltd. They will manage the school filtering, in line with this policy and Online Safety Coordinators will keep records / logs of breaches of the filtering systems.

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

- be logged in change control logs and create log / audit of the change control logs
- be reported to a second responsible person (Online Safety Coordinator) :

All users have a responsibility to report immediately to Online Safety Lead or School Secretary any infringements of the school's filtering policy of which they become aware or any sites that are accessed, which they believe should have been filtered.

Users must not attempt to use any programmes or software that might allow them to bypass the filtering / security systems in place to prevent access to such materials.

Policy Statements

Internet access is filtered for all users. Differentiated internet access is available for staff and customised filtering changes are managed by the school. 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 frequently monitored. The monitoring process alerts the school to breaches of the filtering policy, 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 school network, filtering will be applied that is consistent with school practice.

- *The school has provided enhanced / differentiated user-level filtering through the use of the* Fastvue Reporter *filtering programme.*
- *In the event of the technical staff needing to switch off the filtering for any reason, or for any user, this must be logged and carried out by a process that is agreed by the Headteacher/Head of School.*
- *Mobile devices that access the school internet connection (whether school or personal devices) will be subject to the same filtering standards as other devices on the school systems*
- *Any filtering issues should be reported immediately to the filtering provider.*

Requests from staff for sites to be removed from the filtered list will be considered by the technical staff (Online Safety Lead and Glyn Pascoe) for educational reasons only. *If the request is agreed, this action will be recorded and logs of such actions shall be reviewed regularly by the Online Safety Group*

Education / Training / Awareness

Pupils will be made aware of the importance of filtering systems through the online safety education programme. They will also be warned of the consequences of attempting to subvert the filtering system. Staff users will be made aware of the filtering systems through:

- the Acceptable Use Agreement
- induction training
- staff meetings, briefings, Inset.

Parents will be informed of the school's filtering policy through the Acceptable Use Agreement and through online safety awareness sessions, newsletters, twitter and the school website.

Users who gain access to, or have knowledge of others being able to access, sites which they feel should be filtered (or unfiltered) should report this in the first instance to their school Online Safety Coordinator who will decide whether to make school level changes.

Monitoring

No filtering system can guarantee 100% protection against access to unsuitable sites. The school will therefore monitor the activities of users on the school network and on school equipment as indicated in the School Online Safety Policy and the Acceptable Use Agreement. *Monitoring will take place as follows:* Fastvue email alerts will be sent to the school's Online Safety Coordinator, School Secretary and Headteacher/Head of School containing details of the adult and profanity search.

Audit / Reporting

Logs of filtering change controls and of filtering incidents will be made available to:

- the responsible person – the school's Online Safety Coordinator
- Online Safety Group
- Online Safety Governor / Governors committee
- External Filtering provider / Local Authority / Police on request

The filtering policy will be reviewed in the response to the evidence provided by the audit logs of the suitability of the current provision.

Social Media Policy

Policy Updated: July 2021

Policy Approved: ……………………

Policy Review Date: July 2022

Social media (e.g. Facebook, Twitter, Instagram, LinkedIn) is a broad term for any kind of online platform which enables people to directly interact with each other. However, some games, for example Minecraft or World of Warcraft and video sharing platforms such as YouTube have social media elements to them.

The school recognises the numerous benefits and opportunities which a social media presence offers. Staff, parents/carers and pupils/students are actively encouraged to find creative ways to use social media. However, there are some risks associated with social media use, especially around the issues of safeguarding, bullying and personal reputation. This policy aims to encourage the safe use of social media by *the Rainbow MAT schools*, it's staff, parents, carers and children.

Scope

This policy is subject to the school's Codes of Conduct and Acceptable Use Agreements.

This policy:

- Applies to all staff and to all online communications which directly or indirectly, represent the school.
- Applies to such online communications posted at any time and from anywhere.
- Encourages the safe and responsible use of social media through training and education
- *Defines the monitoring of public social media activity pertaining to the school*

The school respects privacy and understands that staff and pupils/students may use social media forums in their private lives. However, personal communications likely to have a negative impact on professional standards and/or the school's reputation are within the scope of this policy.

Professional communications are those made through official channels, posted on a school account or using the school name. All professional communications are within the scope of this policy.

Personal communications are those made via a personal social media accounts. In all cases, where a personal account is used which associates itself with the school or impacts on the school, it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy.
Personal communications which do not refer to or impact upon the school are outside the scope of this policy.

Digital communications with students are also considered. *Staff may use social media to communicate with learners via a school social media account for teaching and learning purposes but must consider whether this is appropriate and consider the potential implications.*

Organisational control

Roles & Responsibilities

- SLT

    - Facilitating training and guidance on Social Media use.
    - Developing and implementing the Social Media policy
    - Taking a lead role in investigating any reported incidents.
    - Making an initial assessment when an incident is reported and involving appropriate staff and external agencies as required.
    - Receive completed applications for Social Media accounts
    - Approve account creation
- Administrator / Moderator
    - Create the account following SLT approval
    - Store account details, including passwords securely
    - Be involved in monitoring and contributing to the account
    - Control the process for managing an account after the lead staff member has left the organisation (closing or transferring)
- Staff
    - Know the contents of and ensure that any use of social media is carried out in line with this and other relevant policies
    - Attending appropriate training
    - Regularly monitoring, updating and managing content he/she has posted via school accounts
    - Adding an appropriate disclaimer to personal accounts when naming the school

Process for creating new accounts
The school community is encouraged to consider if a social media account will help them in their work, e.g. a history department Twitter account, or a "Friends of the school" Facebook page. Anyone wishing to create such an account must present a business case to the School Leadership Team which covers the following points:-

- The aim of the account
- The intended audience
- How the account will be promoted
- Who will run the account (at least two staff members should be named)
- Will the account be open or private/closed

Following consideration by the SLT an application will be approved or rejected. In all cases, the SLT must be satisfied that anyone running a social media account on behalf of the school has read and understood this policy and received appropriate training. This also applies to anyone who is not directly employed by the school, including volunteers or parents.

Monitoring

School accounts must be monitored regularly and frequently (preferably 7 days a week, including during holidays). Any comments, queries or complaints made through those accounts must be responded to within 24 hours (or on the next working day if received at a weekend) even if the response is only to acknowledge receipt. Regular monitoring and intervention is essential in case a situation arises where bullying or any other inappropriate behaviour arises on a school social media account.

Behaviour

- The school requires that all users using social media adhere to the standard of behaviour as set out in this policy and other relevant policies.
- Digital communications by staff must be professional and respectful at all times and in accordance with this policy. Staff will not use social media to infringe on the rights and privacy of others or make ill-considered comments or judgments about staff. School social media accounts must not be used for personal gain. Staff must ensure that confidentiality is maintained on social media even after they leave the employment of the school.
- Users must declare who they are in social media posts or accounts. Anonymous posts are discouraged in relation to school activity.
- If a journalist makes contact about posts made using social media staff must follow the school media policy before responding.
- Unacceptable conduct, (e.g. defamatory, discriminatory, offensive, harassing content or a breach of data protection, confidentiality, copyright) will be considered extremely seriously by the school and will be reported as soon as possible to a relevant senior member of staff, and escalated where appropriate.
- The use of social media by staff while at work may be monitored, in line with school policies. *The Rainbow MAT permits reasonable and appropriate access to private social media sites. However, where excessive use is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken*
- The Rainbow MAT will take appropriate action in the event of breaches of the social media policy. Where conduct is found to be unacceptable, the school will deal with the matter internally. Where conduct is considered illegal, the school will report the matter to the police and other relevant external agencies, and may take action according to the disciplinary policy.

Legal considerations

- Users of social media should consider the copyright of the content they are sharing and, where necessary, should seek permission from the copyright holder before sharing.
- Users must ensure that their use of social media does not infringe upon relevant data protection laws, or breach confidentiality.

Handling abuse

- When acting on behalf of a Rainbow MAT school, handle offensive comments swiftly and with sensitivity.
- If a conversation turns and becomes offensive or unacceptable, school users should block, report or delete other users or their comments/posts and should inform the audience exactly why the action was taken
- If you feel that you or someone else is subject to abuse by colleagues through use of a social networking site, then this action must be reported using the agreed Rainbow MAT protocols.

Tone

The tone of content published on social media should be appropriate to the audience, whilst retaining appropriate levels of professional standards. Key words to consider when composing messages are:

- Engaging
- Conversational
- Informative
- Friendly (on certain platforms, e.g. Facebook)

Use of images

Rainbow MAT use of images can be assumed to be acceptable, providing the following guidelines are strictly adhered to.

- Permission to use any photos or video recordings should be sought in line with the Rainbow MAT's digital and video images policy. If anyone, for any reason, asks not to be filmed or photographed then their wishes should be respected.
- Under no circumstances should staff share or upload student pictures online other than via school owned social media accounts
- Staff should exercise their professional judgement about whether an image is appropriate to share on school social media accounts. Students should be appropriately dressed, not be subject to ridicule and must not be on any school list of children whose images must not be published.
- If a member of staff inadvertently takes a compromising picture which could be misconstrued or misused, they must delete it immediately.

Personal use

- Staff
    - Personal communications are those made via a personal social media accounts. In all cases, where a personal account is used which associates itself with the school or impacts on the school, it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy.
    - Personal communications which do not refer to or impact upon the school are outside the scope of this policy.
    - Where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken
    - *The Rainbow MAT permits reasonable and appropriate access to private social media sites.*
- Pupil/Students
    - Staff are not permitted to follow or engage with current or prior pupils/students of the school on any personal social media network account.
    - The school's education programme should enable the pupils to be safe and responsible users of social media.
    - Pupils are encouraged to comment or post appropriately about the school. Any offensive or inappropriate comments will be resolved by the use of the school's behaviour policy
- Parents/Carers
    - If parents/carers have access to a school learning platform where posting or commenting is enabled, parents/carers will be informed about acceptable use.

  - The school has an active parent/carer education programme which supports the safe and positive use of social media. This includes information on the website.
  - Parents/Carers are encouraged to comment or post appropriately about the school. In the event of any offensive or inappropriate comments being made, the school will ask the parent/carer to remove the post and invite them to discuss the issues in person. If necessary, refer parents to the school's complaints procedures.

Monitoring posts about a Rainbow MAT school

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

Appendix

Managing your personal use of Social Media:

- "Nothing" on social media is truly private
- Social media can blur the lines between your professional and private life. Don't use the Rainbow MAT school logo and/or branding on personal accounts
- Check your settings regularly and test your privacy
- Keep an eye on your digital footprint
- Keep your personal information private
- Regularly review your connections – keep them to those you want to be connected to
- When posting online consider; Scale, Audience and Permanency of what you post
- If you want to criticise, do it politely.
- Take control of your images – do you want to be tagged in an image? What would children or parents say about you if they could see your images?
- Know how to report a problem

Managing school social media accounts

The Do's

- Check with a senior leader before publishing content that may have controversial implications for the school
- Use a disclaimer when expressing personal views
- Make it clear who is posting content
- Use an appropriate and professional tone
- Be respectful to all parties
- Ensure you have permission to 'share' other peoples' materials and acknowledge the author
- Express opinions but do so in a balanced and measured manner
- Think before responding to comments and, when in doubt, get a second opinion
- Seek advice and report any mistakes using the school's reporting process
- Consider turning off tagging people in images where possible

The Don'ts

- Don't make comments, post content or link to materials that will bring the Rainbow MAT into disrepute
- Don't publish confidential or commercially sensitive material
- Don't breach copyright, data protection or other relevant legislation
- Consider the appropriateness of content for any audience of school accounts, and don't link to, embed or add potentially inappropriate content
- Don't post derogatory, defamatory, offensive, harassing or discriminatory content
- Don't use social media to air internal grievances

Acknowledgements

With thanks to Rob Simmonds of Well Chuffed Comms (wellchuffedcomms.com) and Chelmsford College for allowing the use of their policies in the creation of this policy.

The Rainbow Multi Academy Trust

Building a Brighter Future...

Twitter Policy

Policy Updated: July 2021

Policy Approved: ……………………

Policy Review Date: July 2022

What is Twitter?

Twitter is a form of social media which allows users to send and read 140-character messages or 'Tweets'. These might be simple messages or announcements or may include pictures or links to other sites on the internet. Users access Twitter either through the website (there is a link and feed to this on www.troon.cornwall.sch.uk) or by using the app on a mobile device (e.g. an iPad/iPhone or Android equivalent). Tweets can be viewed via the internet without signing up or users can create a Twitter account to 'follow' certain people or organisations. Troon CP School recognises that access to class/school Twitter accounts gives pupils and staff greater opportunities to learn, engage, communicate and develop skills that will prepare them for work, life and citizenship.

Why use Twitter in school?

Many UK schools are using Twitter, Troon School have successfully trialled 3 accounts @TroonSchool, @BeechTroon and @HollyTroon. The uses of Twitter are endless but some examples include:

- Celebrating achievement – of individuals, teams and the whole school.
- Collaborating with pupils and teachers in other schools.
- Updating the school community about school events and news (including links to our school website).
- Engaging our pupils by connecting with people all over the world including authors, industry experts, scientists, sports people and astronauts.
- Engaging the whole school community in discussion about what matters in our school.
- Giving our pupils an insight into, and stimulating conversation about, events and issues around the world that matter to them.

Troon CP School Twitter handles

@TroonSchool	whole school account
@SquirrelsTroon	nursery
@HedgehogsTroon	reception class
@Willow_Troon	year 1
@BeechTroon	year 2
@HazelTroon	year 3
@OakTroon	year 4 / 5
@MapleTroon	year 5 (currently out of use as no y5 class)
@HollyTroon	year5 / 6

Penponds School Twitter Handles

@Penponds_School	whole school account
@CarnBrea_PP	reception class
@Godolphin_PP	year1/2 class
@Trencom_PP	year 3/4 class
@Tregonning_PP	year5/6 class

St Meriadoc Infants Twitter Handles

St Meriadoc Junior Twitter Handles

@StMeriadoc	whole school account

Rainbow MAT CEO Twitter Handle

@RainbowMATcrwll	Samantha Jones

Is it safe?

We strongly believe that part of our role in the technological age we are learning in is to educate our pupils to use forms of social media such as Twitter effectively and safely. Tweets will only be posted by adults in school and anyone who the school or class choose to follow will be closely scrutinised beforehand to assess their suitability.

Aims of Using Twitter:

To share and celebrate children's achievements and successes
To allow our pupils to connect with the world
To demonstrate safe and responsible use of social media
To update the school community on a range of issues
To encourage the use of 21st Century technology

- The school and class Twitter accounts will be public accounts. The online safety coordinator will monitor school and class followers and block those who appear to not be school focused.

- Class Twitter will only ever be controlled by teachers working at Rainbow MAT. Pupils will have the chance to write Tweets and help select who their class 'follows' but both of these will always be vetted by teaching staff beforehand. Twitter users must be 13+ years of age.

- Class Twitter accounts will only follow other accounts that teaching staff agree are both suitable (based both on knowledge of the account holder and from previous 'Tweets') and of educational merit.

- School / Class Twitter accounts will never include named photos and names of pupils in the same Tweet (it will be either / or). Parents have the right to request for their child not to appear in any Tweets either by name of photo, such requests should be made in writing through the school office or their child's Class Teacher.

- The Rainbow MAT community uses Twitter with a firm knowledge of the potential dangers associated with social networking. This means that Class Teachers take every opportunity to discuss safety issues related to the use of Twitter and model these in their use of all forms of ICT.

- Class/school Twitter accounts will be in the Public domain. So while tweets and comments from parents and followers are actively encouraged; inappropriate language or photographs may result in an account being blocked by the school.

- We make all efforts to ensure pupils' safety and security online, but will not be held accountable for any harm or damages that result from misuse of a class/school Twitter account.

- Staff should avoid using their own equipment to tweet in school unless learning off-site and need to use an alternative internet connection to send a class/school tweet - for school purposes only.

- Class Twitter handles to be updated with new class names when appropriate.

- Twitter's help center can be found at https://help.twitter.com/

What is inappropriate content and referencing and how it will be dealt with?

Our school welcomes any referencing, mentions or interactions that promote the school in a positive light only. Therefore, Rainbow MAT deems any of the following as inappropriate:

- Offensive language or comments aimed at the school, its staff, parents, governors or others affiliated with the school.
- Unsuitable images or content posted into its feed.
- Unsuitable images or content finding its way from another's account into our school Twitter accounts.
- Images or text that infringes upon copyright.
- Comments that undermine the school, its staff, parents, governors or others affiliated with the school.

Any inappropriate content will be deleted and its users will be removed, blocked and depending on the comment reported to Twitter. Incidents of a more serious nature may be reported to the appropriate authority.

Guide to Twitter

Tweet: A 140-character message.

Retweet (RT): 'Quoting' or reposting someone else's tweet you think might be of interest to others. RT usually precedes the original post to give credit to the user who published it first. (Source: @UKEdChat)

Feed The stream of tweets you see on your homepage. It's comprised of updates from users you follow.

Handle Your username (e.g. '@TroonSchool')

Mention/Reply(@) A way to reference another user by their username in a tweet. Users are notified when @mentioned. It's a way to conduct discussions with other users. If you are replying to a tweet and want everyone to see your response, place a full-stop/period prior to the user name .@ukedchat

Hashtag (#) A way to denote a topic of conversation or participate in a larger linked discussion (e.g. #edchat). You can also click on a hashtag to see all the tweets that mention it in real time — even from people you don't follow.

DM This is a private Direct Message sent to a twitter user. You must follow that user before you can message them. DMs don't appear in the public twitter stream.

Follow These are the accounts you are following and the tweets will appear in your time-line.

Follower Someone who follows you and your tweets. Be grateful for any feedback.

Link Including a URL in your tweet. You can use shortened URL services, such as bit.ly although twitter mainly shortens URLs automatically now.

Getting started . . .

1. Create an account – decide on your 'handle' (e.g. @TroonSchool), upload a photo and add a short 'bio' so people have an idea of who you are (e.g. 'We are Holly Class, a year 5/6 class at Troon CP School).

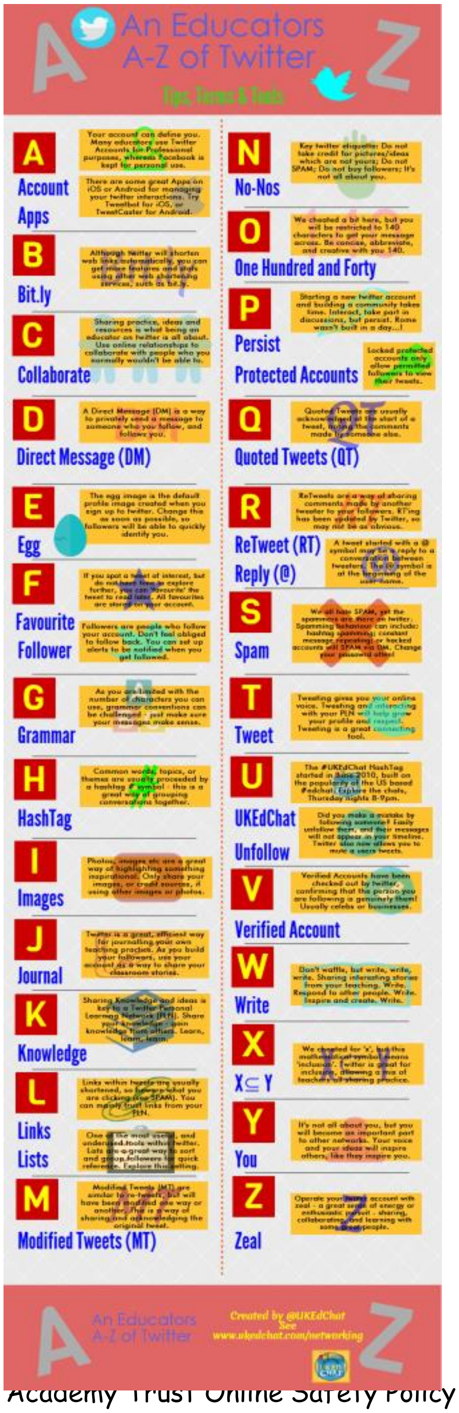
2. Decide who to follow – you can find other Twitter uses to begin with by using the search function. Once you've found who you're looking for, simply click 'follow' and all their Tweets will automatically appear on your 'feed' (your feed is part of the Twitter app or website so you will not be notified of other people's Tweets (like you might a text message for example) unless you request this for any user you are following).

Who you follow is clearly down to what you want to get out of the Twitter experience. Many classes choose to follow various authors or poets; others find it a really use tool for keeping informed on various issues by following other classes, schools and organisations such as NASA. Once you are following a number of other users, Twitter will become more intuitive in suggesting others that might be of interest.

3. Tweet! – Start small with simple messages, gradually including hashtags such as #maths in each of your tweets. As you are limited with the number of characters you can use, grammar conventions can be challenged - just make sure your messages make sense. Find a class from another school and share # to interact with each other.

A popular way to enter the Twitter for the first time is to 'Retweet' a comment from someone else. This is a bit like quoting someone else and will be done primarily because you want people who follow you to see it. It will appear on your personal feed but with the original author credited with the Tweet.
For lots more information visit https://help.twitter.com/en

Twitter infographic - http://ukedchat.com/2014/06/16/resource-an-a-z-of-twitter-for-educators/



An Educators A-Z of Twitter

Tips, Terms & Tools

A
Account – Your account can define you. Many educators use Twitter Accounts for Professional purposes, whereas Facebook is kept for personal use.
Apps – There are some great Apps on iOS or Android for managing your twitter interactions. Try Tweetbot for iOS, or TweetCaster for Android.

B
Bit.ly – Although twitter will shorten web links automatically, you can get more features and stats using other web shortening services, such as bit.ly.

C
Collaborate – Sharing practice, ideas and resources is what being an educator on twitter is all about. Use online relationships to collaborate with people who you normally wouldn't be able to.

D
Direct Message (DM) – A Direct Message (DM) is a way to privately send a message to someone who you follow, and follows you.

E
Egg – The egg image is the default profile image created when you sign up to twitter. Change this as soon as possible, so followers will be able to quickly identify you.

F
Favourite – If you spot a tweet of interest, but do not have time to explore further, you can 'favourite' the tweet to read later. All favourites are stored on your account.
Follower – Followers are people who follow your account. Don't feel obliged to follow back. You can set up alerts to be notified when you get followed.

G
Grammar – As you are limited with the number of characters you can use, grammar conventions can be challenged - just make sure your messages make sense.

H
HashTag – Common words, topics, or themes are usually proceeded by a hashtag # symbol - this is a great way of grouping conversations together.

I
Images – Photos, images etc are a great way of highlighting something inspirational. Only share your images, or credit sources, if using other images or photos.

J
Journal – Twitter is a great, efficient way for journalling your own teaching practice. As you build your followers, use your account as a way to share your classroom stories.

K
Knowledge – Sharing Knowledge and ideas is key to a Twitter Personal Learning Network (PLN). Share your knowledge - gain knowledge from others. Learn, learn, learn.

L
Links – Links within tweets are usually shortened, so beware what you are clicking (see SPAM). You can mainly trust links from your PLN.
Lists – One of the most useful, and underused tools within twitter. Lists are a great way to sort and group followers for quick reference. Explore this setting.

M
Modified Tweets (MT) – Modified Tweets (MT) are similar to re-tweets, but will have been modified one way or another. This is a way of sharing and acknowledging the original tweet.

N
No-Nos – Key twitter etiquette: Do not take credit for pictures/ideas which are not yours; Do not SPAM; Do not buy followers; It's not all about you.

O
One Hundred and Forty – We cheated a bit here, but you will be restricted to 140 characters to get your message across. Be concise, abbreviate, and creative with you 140.

P
Persist – Starting a new twitter account and building a community takes time. Interact, take part in discussions, but persist. Rome wasn't built in a day...!
Protected Accounts – Locked protected accounts only allow permitted followers to view their tweets.

Q
Quoted Tweets (QT) – Quoted Tweets are usually acknowledged at the start of a tweet, noting the comments made by someone else.

R
ReTweet (RT) – ReTweets are a way of sharing comments made by another tweeter to your followers. RT'ing has been updated by Twitter, so may not be as obvious.
Reply (@) – A tweet started with a @ symbol may be a reply to a conversation between tweeters. The @ symbol is at the beginning of the user-name.

S
Spam – We all hate SPAM, yet the spammers are there on twitter. Spamming behaviour can include: hashtag spamming; constant message repeating; or hacked accounts will SPAM via DM. Change your password often!

T
Tweet – Tweeting gives you your online voice. Tweeting and interacting with your PLN will help grow your profile and respect. Tweeting is a great connecting tool.

U
UKEdChat – The #UKEdChat HashTag started in June 2010, built on the popularity of the US based #edchat. Explore the chats, Thursday nights 8-9pm.
Unfollow – Did you make a mistake by following someone? Easily unfollow them, and their messages will not appear in your timeline. Twitter also now allows you to mute a users tweets.

V
Verified Account – Verified Accounts have been checked out by twitter, confirming that the person you are following is genuinely them! Usually celebs or businesses.

W
Write – Don't waffle, but write, write, write. Sharing interesting stories from your teaching. Write. Respond to other people. Write. Inspire and create. Write.

X
$X \subseteq Y$ – We cheated for 'x', but this mathematical symbol means 'inclusion'. Twitter is great for inclusion, allowing a mix of teachers all sharing practice.

Y
You – It's not all about you, but you will become an important part to other networks. Your voice and your ideas will inspire others, like they inspire you.

Z
Zeal – Operate your twitter account with zeal - a great sense of energy or enthusiastic pursuit - sharing, collaborating and learning with some great people.

An Educators A-Z of Twitter

Created by @UKEdChat
See
www.ukedchat.com/networking

The Rainbow Multi Academy Trust

Building a Brighter Future...

Blogging Policy

Policy Updated: July 2021

Policy Approved: ……………………

Policy Review Date: July 2022

Taken from David Mitchell

Twitter: @DeputyMitchell

Aims and Objectives

Whilst blogging has been around for 10+ years, more and more schools are now giving their pupils a voice and an audience through blogging. These are mainly in the form of class blogs but can also be in the form of project blogs or individual pupil blogs. Whilst there are many blogging platforms, Wordpress is the most popular. The school currently has an account with eschools.

This policy will outline the safe management of setting up and running a blogging platform. A successful blog can:

→ Safely give your pupils a wider audience for their learning.

→ Encourage reluctant learners to participate and succeed

→ Allow pupils to receive feedback safely from many different people

→ Allow your pupils to peer assess each other's learning

→ Encourage parental engagement

→ Provide a platform that you can embed Web2.0/3.0 tools into

→ Promote your pupils' learning across the globe

Online Safety

Blogging involves pupils working on a blog whilst in school and also at home. To be able to post, pupils need to log into the blog either using an individual sign in or a class sign in. The advantages of individual sign in is that this gives more ownership to each pupil. Most blog platforms allow accounts to have different permissions. Contributor is the lowest level that allows a user to post. A contributor can submit a post for review, however, this will need to be authorised by the admin before it appears on the blog. The 'Contributor' permission level is recommended for Primary School. Any other permission level above that of 'Contributor' will allow posts to be viewable as soon as the pupil clicks 'Submit'.

Rainbow MAT has sought permission for each child to have access to their class blog to display the learning from each pupil and has sought permission for the photographs of each pupil to be displayed on a blog. Names will not appear alongside images of pupils unless additional permission has been sought by the class teacher.

Blog Rules:

Using a blog safely is the most important thing about being a blogger. The following rules, if followed, will minimise any risks and will ensure that you will stay safe whilst blogging.

Don'ts:

1. Never give away any personal information about your location or identity.
2. Don't post pictures of yourself without specific permission from your teacher or parents.
3. Never give out your log in details to anyone.
4. Don't use text language in your posts

Do's:

1. Post about whatever you like.
2. If you receive a comment, it is polite to respond, say thank you and reply to a question if they have left one.
3. Comment on other people's posts too. Blogging is about commenting and posting!
4. If your post doesn't appear straight away, your teacher might be busy, do be patient.
5. Try to post about things that your audience would like to read.
6. If you see anything that shouldn't be on your screen, do tell your teacher or parents immediately.
7. Do visit other class blogs regularly to read and comment. This helps people come back to your blog.
8. Try to show off your best work/writing whilst blogging and use the tips people suggest to you to improve.
9. Always tag your posts with your first name and include key words specific to your post.

The Role of the Blog Admin/Teacher:

The blog admin normally is the class teacher. This responsibility as gatekeeper is key to ensuring safety for the pupils using the blog. The following guidelines should be followed if a successful flowing blog is to be achieved:

1. Visit the blog regularly. It is better to visit short and often than catching up once a week. Your bloggers will appreciate comments and posts being approved quickly!
2. If you use a shared computer, log out at the end of each session.
3. Promote the links on the class blog to the parents and the wider community. Twitter is a great way to promote a blog.
4. A blog can take a while to gather momentum and an audience. Be patient... the audience will come!
5. Your users will need to log in. For a quick solution, you can have one Username and Password for your class to get posts on the blog. However, for older pupils of 7+ they are more than capable of having their own log in.
6. The safest permission setting for your blogger is 'Contributor'. This will allow them to log in and post but the blog admin will need to approve each post.
7. Mention the blog in assemblies and have it on display at parent evenings or school events, a blogging culture will soon be established!
8. Make sure each blog looks different in your school. This will help keep the interest high for the pupils from year to year.
9. Visit other blogs regularly and promote these to your class through links on your blog. What goes around comes around with blogging and strong loyal communities will form quickly.
10. Try using a free project like Quadblogging. This will give your pupils a quick audience. See http://quadblogging.net for more details.

Resources

SWGfL has produced a wide range of information leaflets and teaching resources, including films and video clips – for parents and school staff. A comprehensive list of these resources (and those available from other organisations) is available on the "SWGfL Safe" website:

http://www.swgfl.org.uk/safety/safetyresources.asp?page=schoolst_resources&audienceid=3

Links to other resource providers:

BBC Chatguides: http://www.bbc.co.uk/chatguide/index.shtml

Kidsmart: http://www.kidsmart.org.uk/default.aspx

Know It All - http://www.childnet-int.org/kia/

Cybersmart - http://www.cybersmartcurriculum.org/home/

NCH - http://www.stoptextbully.com/

Chatdanger - http://www.chatdanger.com/

Internet Watch Foundation: http://www.iwf.org.uk/media/literature.htm

Digizen – cyber-bullying films: http://www.digizen.org/cyberbullying/film.aspx

London Grid for Learning: http://cms.lgfl.net/web/lgfl/safety/resources

Legislation

Schools should be aware of the legislative framework under which this Online Safety Policy template and guidance has been produced. It is important to note that in general terms an action that is illegal if committed offline is also illegal if committed online.

It is recommended that legal advice is sought in the advent of an e safety issue or situation.

Computer Misuse Act 1990

This Act makes it an offence to:

- Erase or amend data or programs without authority;
- Obtain unauthorised access to a computer;
- "Eavesdrop" on a computer;
- Make unauthorised use of computer time or facilities;
- Maliciously corrupt or erase data or programs;
- Deny access to authorised users.

Data Protection Act 1998

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

- Fairly and lawfully processed.
- Processed for limited purposes.
- Adequate, relevant and not excessive.
- Accurate.
- Not kept longer than necessary.
- Processed in accordance with the data subject's rights.
- Secure.
- Not transferred to other countries without adequate protection.

Freedom of Information Act 2000

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

Communications Act 2003

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

Malicious Communications Act 1988

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

Regulation of Investigatory Powers Act 2000

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

- Establish the facts;
- Ascertain compliance with regulatory or self-regulatory practices or procedures;
- Demonstrate standards, which are or ought to be achieved by persons using the system;
- Investigate or detect unauthorised use of the communications system;
- Prevent or detect crime or in the interests of national security;
- Ensure the effective operation of the system.
- Monitoring but not recording is also permissible in order to:
- Ascertain whether the communication is business or personal;
- Protect or support help line staff.
- The school reserves the right to monitor its systems and communications in line with its rights under this act.

Trade Marks Act 1994

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

Copyright, Designs and Patents Act 1988

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

Telecommunications Act 1984

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

Criminal Justice & Public Order Act 1994

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

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

Racial and Religious Hatred Act 2006

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

Protection from Harassment Act 1997

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

Protection of Children Act 1978

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

Sexual Offences Act 2003

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

Public Order Act 1986

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

Obscene Publications Act 1959 and 1964

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

Human Rights Act 1998

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

- The right to a fair trial
- The right to respect for private and family life, home and correspondence
- Freedom of thought, conscience and religion
- Freedom of expression
- Freedom of assembly
- Prohibition of discrimination
- The right to education

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

The Education and Inspections Act 2006

Empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of students / pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour.

The Education and Inspections Act 2011

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

The Protection of Freedoms Act 2012

Requires schools to seek permission from a parent / carer to use Biometric systems
The School Information Regulations 2012
Requires schools to publish certain information on its website:
https://www.gov.uk/guidance/what-maintained-schools-must-publish-online

Serious Crime Act 2015

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

The Rainbow Multi Academy Trust

Building a Brighter Future...

Online Bullying Policy

Policy Updated: July 2021

Policy Approved: ....

Policy Review Date: July 2022

Adapted from Cornwall Council

ONLINE BULLYING

What is online bullying?

"Online bullying is an aggressive, intentional act carried out by a group or individual, using electronic forms of contact, repeatedly over time against a victim who cannot easily defend him or herself."[2]

Seven categories of online bullying have been identified:

- Text message bullying involves sending unwelcome texts that are threatening or cause discomfort.
- Picture/video-clip bullying via mobile phone cameras is used to make the person being bullied feel threatened or embarrassed, with images usually sent to other people. 'Happy slapping' involves filming and sharing physical attacks.
- Phone call bullying via mobile phone uses silent calls or abusive messages. Sometimes the bullied person's phone is stolen and used to harass others, who then think the phone owner is responsible. As with all mobile phone bullying, the perpetrators often disguise their numbers, sometimes using someone else's phone to avoid being identified.
- Email bullying uses email to send bullying or threatening messages, often using a pseudonym for anonymity or using someone else's name to pin the blame on them.
- Chat room bullying involves sending menacing or upsetting responses to children or young people when they are in a web-based chat room.
- Bullying through instant messaging (IM) is an Internet-based form of bullying where children and young people are sent unpleasant messages as they conduct real-time conversations online.
- Bullying via websites includes the use of defamatory blogs (web logs), personal websites and online personal polling sites. There has also been a significant increase in social networking sites for young people, which can provide new opportunities for online bullying.

What can schools do about it?

While other forms of bullying remain prevalent, online bullying is already a significant issue for many young people. Rainbow MAT recognise that staff, parents and children need to work together to prevent this and to tackle it whenever it occurs.

CEOs, School Governors, Headteachers/Head of Schools and schools have a duty to ensure that:
bullying via mobile phone or the Internet is included in their mandatory anti-bullying policies, that these policies are regularly updated, and that teachers have sufficient knowledge to deal with online bullying in school[3].

The Rainbow MAT ensures that:

- the curriculum teaches pupils about the risks of new communications technologies, the consequences of their misuse, and how to use them safely including personal rights
- all e-communications used on the school site or as part of school activities off-site are monitored
- clear policies are set about the use of mobile phones at school and at other times when young people are under the school's authority
- Internet blocking technologies are continually updated and harmful sites blocked
- they work with pupils and parents to make sure new communications technologies are used safely, taking account of local and national guidance and good practice

[2] Research commissioned by the Anti-Bullying Alliance from Goldsmiths College, University of London

[3] The School Standards and Framework Act 1998 require schools to have anti bullying policies; the anti bullying policy should include or refer to a online bullyingpolicy. The ICT policy should also refer to cbyerbullying

- security systems are in place to prevent images and information about pupils and staff being accessed improperly from outside school
- they work with police and other partners on managing online bullying.

ICT and Mobile Phone Policy

If an online bullying incident directed at a child occurs using e-mail or mobile phone technology, either inside or outside school time, the Rainbow MAT will take the following steps:

- Advise the child not to respond to the message
- Refer to relevant policies, e.g. online safety/acceptable use, anti-bullying and PSHE and apply appropriate sanctions
- Secure and preserve any evidence
- Inform the sender's e-mail service provider
- Notify parents of the children involved
- Consider delivering a parent workshop for the school community
- Consider informing the police depending on the severity or repetitious nature of the offence. The school recognises that some activities could be a criminal offence under a range of different laws including: the Protection from Harassment Act 1997; the Malicious Communication Act 1988; section 127 of the Communications Act 2003 and the Public Order Act 1986
- Inform the SWG4L lead: Jane McFall: 01872 322765

If malicious or threatening comments are posted on an Internet site or Social Networking Site about a pupil of member of staff, the Rainbow MAT will also:

- Inform and request that the comments be removed if the site is administered externally
- Secure and preserve any evidence
- Send all the evidence to www.ceop.gov.uk/contact_us.html if of a sexual nature
- Endeavour to trace the origin and inform the police as appropriate.
- Inform the SWG4L lead: Jane McFall 01872 322765

Working with Parents

The Rainbow MAT will develop a home-school agreement that includes clear statements about e-communications. The school seeks to regularly update parents on:

- What to do if problems arise
- E-communication standards and practices in school
- What's being taught in the curriculum
- Supporting parents and pupils if online bullying occurs by:
  - ✓ Assessing the harm done
  - ✓ Identifying those involved
  - ✓ Taking steps to repair harm and to prevent recurrence

Code of Conduct

The Rainbow MAT has developed an ICT acceptable use policy with our pupils.

Links to other organisations or documents

The following links may help those who are developing or reviewing a school online safety policy and creating their online safety provision:

UK Safer Internet Centre

Safer Internet Centre – https://www.saferinternet.org.uk/
South West Grid for Learning - https://swgfl.org.uk/products-services/online-safety/
Childnet – http://www.childnet-int.org/
Professionals Online Safety Helpline - http://www.saferinternet.org.uk/about/helpline
Revenge Porn Helpline - https://revengepornhelpline.org.uk/
Internet Watch Foundation - https://www.iwf.org.uk/
Report Harmful Content - https://reportharmfulcontent.com/

CEOP

CEOP - http://ceop.police.uk/

ThinkUKnow - https://www.thinkuknow.co.uk/

Others

LGfL – Online Safety Resources
Kent – Online Safety Resources page
INSAFE/Better Internet for Kids - https://www.betterinternetforkids.eu/
UK Council for Internet Safety (UKCIS) - https://www.gov.uk/government/organisations/uk-council-for-internet-safety
Netsmartz - http://www.netsmartz.org/

Tools for Schools

Online Safety BOOST – https://boost.swgfl.org.uk/
360 Degree Safe – Online Safety self-review tool – https://360safe.org.uk/
360Data – online data protection self-review tool: www.360data.org.uk
SWGfL Test filtering - http://testfiltering.com/
UKCIS Digital Resilience Framework - https://www.gov.uk/government/publications/digital-resilience-framework

Bullying/Online-bullying/Sexting/Sexual Harassment

Enable – European Anti Bullying programme and resources (UK coordination/participation through SWGfL & Diana Awards) - http://enable.eun.org/
SELMA – Hacking Hate - https://selma.swgfl.co.uk
Scottish Anti-Bullying Service, Respectme - http://www.respectme.org.uk/
Scottish Government - Better relationships, better learning, better behaviour - http://www.scotland.gov.uk/Publications/2013/03/7388
DfE - Cyberbullying guidance - https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/374850/Cyberbullying_Advice_for_Headteachers_and_School_Staff_121114.pdf
Childnet – Cyberbullying guidance and practical PSHE toolkit: http://www.childnet.com/our-projects/cyberbullying-guidance-and-practical-toolkit
Childnet – Project deSHAME – Online Sexual Harrassment
UKSIC – Sexting Resources
Anti-Bullying Network – http://www.antibullying.net/cyberbullying1.htm
Ditch the Label – Online Bullying Charity
Diana Award – Anti-Bullying Campaign

Social Networking

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

Curriculum

SWGfL Evolve - https://projectevolve.co.uk
UKCCIS – Education for a connected world framework
Teach Today – www.teachtoday.eu/
Insafe - Education Resources

Data Protection

360data - free questionnaire and data protection self review tool
ICO Guides for Education (wide range of sector specific guides)
DfE advice on Cloud software services and the Data Protection Act
IRMS - Records Management Toolkit for Schools
NHS - Caldicott Principles (information that must be released)
ICO Guidance on taking photos in schools
Dotkumo - Best practice guide to using photos

Professional Standards/Staff Training

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

Infrastructure/Technical Support

UKSIC – Appropriate Filtering and Monitoring
SWGfL Safety & Security Resources
Somerset - Questions for Technical Support
NCA – Guide to the Computer Misuse Act
NEN – Advice and Guidance Notes

Working with parents and carers

Online Safety BOOST Presentations - parent's presentation
Vodafone Digital Parents Magazine
Childnet Webpages for Parents & Carers
Get Safe Online - resources for parents
Teach Today - resources for parents workshops/education
Internet Matters

Prevent

Prevent Duty Guidance
Prevent for schools – teaching resources
NCA – Cyber Prevent
Childnet – Trust Me

Research

Ofcom –Media Literacy Research

Further links can be found at the end of the UKCIS Education for a Connected World Framework

Glossary of Terms

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

A more comprehensive glossary can be found at the end of the UKCIS Education for a Connected World Framework

Copyright of the SWGfL School Online Safety Policy Templates is held by SWGfL. Schools and other educational institutions are permitted free use of the templates. Any person or organisation wishing to use the document for other purposes should seek consent from SWGfL and acknowledge its use.

Every reasonable effort has been made to ensure that the information included in this template is accurate, as at the date of publication in January 2020. However, SWGfL cannot guarantee its accuracy, nor can it accept liability in respect of the use of the material whether in whole or in part and whether modified or not. Suitable legal/professional advice should be sought if any difficulty arises in respect of any aspect of this new legislation or generally to do with school conduct or discipline.