Sidney Stringer
Multi Academy Trust

E-Safety Policy
December 2017

Development of this Policy

This e-safety policy has been developed by the SSA MAT safeguarding group consisting of Head teachers, safeguarding leads, ICT network and curriculum leads along with Governor, staff and student representation.

Consultation with the whole school community has taken place through a range of formal and informal meetings.

Schedule for Review

This e-safety policy was approved by the Governing Body on:	To be completed
The implementation of this e-safety policy will be monitored by the:	Assistant Principal for e-learning across the MAT
Monitoring will take place at regular intervals:	Annually
The Safeguarding Committee will receive a report on the implementation of the e-safety policy generated by the monitoring group (which will include anonymous details of e-safety incidents) at regular intervals:	Annually
The E-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 e-safety or incidents that have taken place. The next anticipated review date will be:	May 2018

Should serious e-safety incidents take place, the following external persons / agencies should be informed:	Please refer to flow chart at end of document

The school will monitor the impact of the policy using:

- Logs of reported incidents
- Monitoring logs of internet activity (including sites visited)
- Internal monitoring data for network activity
- Surveys / questionnaires of
    - students / pupils
    - parents / carers
    - staff

Scope of the Policy

This policy applies to all members of the Multi-Academy Trust community (including staff, students/pupils, volunteers, parents/carers, visitors, community users) who have access to and are users of MAT ICT systems, both in and out of the Academies/Schools.

Each academy will deal with such incidents within this policy and associated behaviour and will, where known, inform parents/carers of incidents of inappropriate e-safety behaviour that take place outside of the school environment. Each school/academy will report these incidents back to the MAT e-safety group and MAT Safeguarding Committee.

Roles and Responsibilities

The following section outlines the e-safety roles and responsibilities of individuals and groups within the MAT.

Governors:

Governors in each Academy with safeguarding responsibility are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about e-safety incidents and monitoring reports.

Safeguarding Governors for each Academy should:

- regularly attend at the MAT e-safety group
- regularly monitor e-safety incident logs
- report back to the Governing body

Headteacher/Principal and Senior Leaders:

- The Headteacher has a duty of care for ensuring the safety (including e-safety) of members of the school communities, though the day to day responsibility for e-safety will be delegated to the E-Safety Co-ordinator for each Academy working with the Assistant Principal with responsibility for E-Safety within the MAT.
- The Headteacher, Assistant Principal with responsibility for E-Safety within the MAT and (at least) another member of the Senior Leadership should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff (see flow chart on dealing with e-safety incidents)
- The Headteacher/Principal/Senior Leaders are responsible for ensuring that the E-Safety Coordinator/Officer and other relevant staff receive suitable training to enable them to carry out their e-safety roles and to train other colleagues, as relevant.

E-Safety Coordinator:

Each school/academy should have a named member of staff with a day to day responsibility for e-safety; some schools may choose to combine this with the Child Protection/Safeguarding Officer role.

- attends the MAT e-safety group meetings to report any e-safety incidents
- take day to day responsibility for e-safety issues within their Academy and has a leading role in establishing and reviewing the school e-safety policies and documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- provides training and advice for staff
- liaise with the Headteacher who will decide whether to contact a relevant authority
- liaises with school technical staff
- receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments

MAT Network Manager / Technical staff:

The MAT Network Manager is responsible for ensuring:

- that the academy's technical infrastructure is secure and reasonable steps are taken to prevent misuse or malicious attack
- that the academy meets required internal e-safety technical requirements and any Local Authority Guidance that may apply.

- that users may only access the networks, cloud managed systems audited and operated by the Academy and devices through a properly enforced password protection policy
- that they keep up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant
- that the use of the network is regularly monitored in order that any misuse or attempted misuse can be reported to the E-Safety Officer for investigation
- Ensuring that MAT IT systems have a secure password policy with passwords of at least 8 characters in length.

Teaching and Support Staff

are responsible for ensuring that:

- they have an up to date awareness of e-safety matters and of the current academy e-safety policy and practices
- they have read, understood and signed the Staff Acceptable Use Policy (AUP)
- they report any suspected misuse or problem to the E-Safety Officer for investigation
- all school digital communications with students/pupils/parents/carers should adhere to the MAT staff code of conduct
- e-safety issues are embedded in all aspects of the curriculum and other activities – this should be updated regularly to include relevant issues such as grooming and sexting.
- students understand and follow the e-safety and acceptable use policies
- students 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 where internet use is pre-planned students 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

Child Protection Officer

Should be trained in e-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
- cyber-bullying

MAT E-Safety Group

The E-Safety Group provides a consultative group that has wide representation from the academy community, with responsibility for issues regarding e-safety and the monitoring the e-safety policy including the impact of initiatives. The group will also be responsible for regular reporting to the MAT Governing Body.

Members of the MAT E-safety Group will assist the E-Safety Coordinator with:

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

Students:

- are responsible for using the academy digital technology systems in accordance with their understanding of the Student Acceptable Use Policy
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations for their age and ability
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so for their age and ability
- will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking/use of images and on cyber-bullying for their age and ability
- should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the academy's E-Safety Policy covers their actions out of school, if related to their membership of the school for their age and ability

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 way. The academies will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website and information about national / local e-safety campaigns / literature. Parents and carers will be encouraged to support the schools in promoting good e-safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school
- their children's personal device and storage in the academy including mobile phones, iPads and Chromebooks

Community Users

Community Users who access school systems as part of the wider academy provision will be expected to sign a Community User AUP before being provided with access to school systems

MAT E-safety group members

Role	Name	Training – yes/no and in what form
Governor responsible for e-safety		
MAT E-safety co-ordinator	Andrew Walls	
MAT CP Lead		
MAT ICT Network manager	Paul Jones	
Headteacher/leadership representatives from each school		
Sidney Stringer Academy		
Sidney Stringer Primary		
Radford Primary Academy		
Ernesford Grange Community School		
Riverbank Academy		

Student, Parent and Community members

Students	
Parents	
Community	

Policy Statements

Education – students / pupils

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

E-safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages across the curriculum. The e-safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned e-safety curriculum should be provided as part of the tutorial programme, assemblies and the computing curriculum along with other lessons and should be regularly revisited
- Students should be taught in lessons to be critically aware of the materials/content they access on-line and be guided to validate the accuracy of information.
- Students should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Students should be helped to understand the need for the student Acceptable Use Agreement 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 students 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 students 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, students 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 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 e-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 behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

Schools/Academies will therefore seek to provide information and awareness to parents and carers through:

- Curriculum activities
- Letters, newsletters, website

- Parents/Carers evenings
- High profile events / campaigns e.g. Safer Internet Day
- Reference to the relevant web sites / publications e.g. www.swgfl.org.uk www.saferinternet.org.uk/ http://www.childnet.com/parents-and-carers

Education – The Wider Community

Academies will provide opportunities for local community groups/members of the community to gain from the school's e-safety knowledge and experience. This may be offered through the following:

- Providing family learning events in the use of new digital technologies, digital literacy and e-safety
- The school / academy website will provide e-safety information for the wider community

Education & Training – Staff / Volunteers

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

- A planned programme of formal e-safety training will be made available to staff. This will be annually updated and reinforced. An audit of the e-safety training needs of all staff will be carried out regularly.
- All new staff should receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and Acceptable Use Agreements.
- This E-Safety policy and its updates will be presented to and discussed by staff in staff/team meetings/INSET days.
- Guest users will be provided with a dedicated guest user account and usage of this account this will be monitored by the IT Support Staff
- The E-Safety Coordinator/Officer (or other nominated person) will provide advice/guidance/training to individuals as required.

Training – Governors

Governors should take part in e-safety training sessions, with particular importance for those who are members of any sub-committee/group involved in technology/e-safety/health and safety/child protection. This will be through participation in school training/information sessions.

Technical – infrastructure/equipment, filtering and monitoring

The MAT ICT Network team is responsible for ensuring that each school 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 e-safety responsibilities:

- All technical systems will be managed in ways that ensure that the schools meet recommended technical requirements
- There will be regular reviews and audits of the safety and security of each schools technical systems

- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to technical systems and devices.
- All users will be provided with a username and secure password by the MAT ICT network team who will keep an up to date record of users and their usernames. Users are responsible for the security of their username and password and will be required to change their password at regular intervals.
- The administrator passwords for the MAT ICT systems, used by the Network Manager (or other person) must also be available to each Headteacher/Principal and kept in a secure place
- The MAT ICT Network Manager is responsible for ensuring that software licence logs are audited, accurate and, in liaison with the Director of Business and Finance (MAT), up to date and that regular checks are made to reconcile the number of licenses purchased against the number of software installations.
- 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. Requests for filtering changes will be logged on a centralised system and analysed by the Assistant Principal with responsibility for MAT E-Safety. Requests will be catalogued into three categories:

  Category One: The website is a purely educational website and should be unblocked. This will be forwarded to Trust IT Support to unblock within a 24 hour window.

- Category Two: The website is educational but may pose a low level of risk. For example, artwork that may be controversial, a text or video that explores mature themes or a website that some may find slightly offensive. This will be risk assessed and recorded by the Assistant Principal with Responsibility for E-Safety, and may involve consultation with colleagues, to assess whether the risks outweigh the learning benefits and whether special procedures should be put in place to facilitate safe access to the website. This will then be carried out by the MAT IT Support Staff.

- Category Three: The website would involve a serious change to the use of internet access with the Academy, social media use within the Academy or it may pose an exceptional risk but not be dismissable out of hand. Putting a website request in this category should be the responsibility for the Assistant Principal with responsibility for E-Safety within the MAT and should be reviewed at the next E-Safety MAT Committee Meeting.

- Each school has provided enhanced / differentiated user-level filtering (allowing different filtering levels for different ages/stages and different groups of users – staff/pupils/students etc.)
- MAT 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.
- Concerns about child protection and e-safety should be recorded using the established procedures of each Academy and the Child Protection and Safeguarding Policy of each Academy.
  • If security systems are bypassed for a legitimate reason, for example to test the security of Academy systems, this should be logged in the 'E-Safety Incident' file and the Assistant Principal with Responsibility for E-Safety should authorise the request in advance.

- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, workstations, mobile devices etc. from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested for their security in December, April and August each year with reports issued to the Assistant Principal with Responsibility for E-Safety. The school infrastructure and individual workstations are protected by up to date virus software or are devices which are safely sandboxed to prevent malicious programmes running on them.

  • Guests at Academies will be provided with temporary Wi-Fi access using a Guest SSID and PSK. This will be on a VLAN that prohibits access to Academy network drives and the Academy MIS. The PSK of this Wi-Fi SSID should change every month.
- Portable devices owned by an Academy, or the MAT, and given to staff to aid their productivity are for the sole use of the user that they have been allocated to and only for work related activities.
- This policy recognises that there are often pragmatic reasons to install executable files and applications on Academy devices (e.g. conferencing software, web applications for browsers, educational applications on mobile devices). When this needs to be done on a domained Windows device the installation should be done under the supervision or awareness of the MAT IT Manager, and in his absence, the Assistant Principal with responsibility for ICT across the MAT. If a user chooses to do this the application should be developed and come from a reputable source (e.g. an audited application store) or a reputable company.
  • The Academy officially supports data being stored in Academy managed and audited cloud based storage systems (e.g. G Suite and Office365), network drives and remotely accessed via remote desktop. Any personal data held by staff about students or staff (including but not limited to: names, details, educational history, addresses, SEN data, performance data or human resources data) if stored electronically, must be stored in one of the audited systems (above) or an encrypted USB stick. Users can visit MAT IT Support to learn how to encrypt USB sticks and to have a USB stick encrypted. Other files may be stored on unencrypted devices. Support for encrypting USB devices can be arranged via MAT IT Support.
  • Students are not permitted to use USBs and should be directed to cloud based storage systems as their primary means of portable storage.

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students/pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents/carers and students/pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry 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 students 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 e.g. on social networking sites.
- In accordance with guidance from the Information Commissioner's Office, parents/carers are welcome to take videos and digital images of their children at school events for their own personal use.. 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 students in the digital/video images.

- 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 of staff should not be used for such purposes and stored to a school monitored and audited storage system (the school network or Google Suite).
- Care should be taken when taking digital/video images that students are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Students must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include students will be selected carefully and will comply with good practice guidance on the use of such images.
- Students' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of students are published on the school website (list to be compiled from Parent/Carer AUP at the start of each year)
- Student's work can only be published with the permission of the student and parents or carers.

Data Protection

Please refer to the MAT Data Protection Policy which outlines the position of the Sidney Stringer Multi-Academy Trust on Data Protection.

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection.

The MAT must ensure that:

- 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.
- Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.
- All personal data will be fairly obtained in accordance with the "Privacy Notice" and lawfully processed in accordance with the "Conditions for Processing".

- It has a Data Protection Policy
- It is registered as a Data Controller for the purposes of the Data Protection Act (DPA)

Staff must ensure that they:

- At all times take care to ensure the safe keeping 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 in which they are using personal data.
- Transfer data using encryption and secure password protected devices.

Communications

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

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

- The official academy email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored.
- Users must immediately report, to the nominated person – in accordance with the MAT policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Any digital communication between staff and students or parents/carers (email, chat, messaging etc.) must be professional in tone and content and carried out on an Academy monitored system. These communications may only take place on official (monitored) academy systems. Personal email addresses, text messaging or social media must not be used for these communications. Students should use their Academy e-mail accounts for professional correspondence with staff and not personal accounts.
- Students should be taught about e-safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
- Personal information should not be posted on the academy website and only official email addresses should be used to identify members of staff.

Social Media - Protecting Professional Identity

Expectations for teachers' professional conduct are set out in 'Teachers Standards 2012'. Ofsted's e-safety framework 2012, reviews how a school protects and educates staff and pupils in their use of technology, including what measures would be expected to be in place to intervene and support should a particular issue arise.

The MAT has a duty of care to provide a safe learning environment for pupils and staff. The schools and local authorities could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, cyberbully, discriminate on the grounds of sex, race or disability or who defame a third party may render the academy or local authority liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school through limiting access to personal information:

- 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

School staff should ensure that:

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

Each school's use of social media for professional purposes will be checked regularly by the e-safety working group to ensure compliance with the Social Media, Data Protection, Communications, Digital Image and Video Policies.

Unsuitable / inappropriate activities

The school 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 school policy restricts usage as follows:

User Actions

Acceptable	Acceptable at certain	Acceptable for nominated users	Unacceptable	Unacceptable and illegal

			times			
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	**Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978**					X
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					X
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					X
	criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986					X
	pornography				X	
	promotion of any kind of discrimination				X	
	threatening behaviour, including promotion of physical violence or mental harm				X	
	any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				X	
Using school systems to run a private business					X	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school / academy					X	
Infringing copyright					X	
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)					X	
Creating or propagating computer viruses or other harmful files					X	
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)					X	

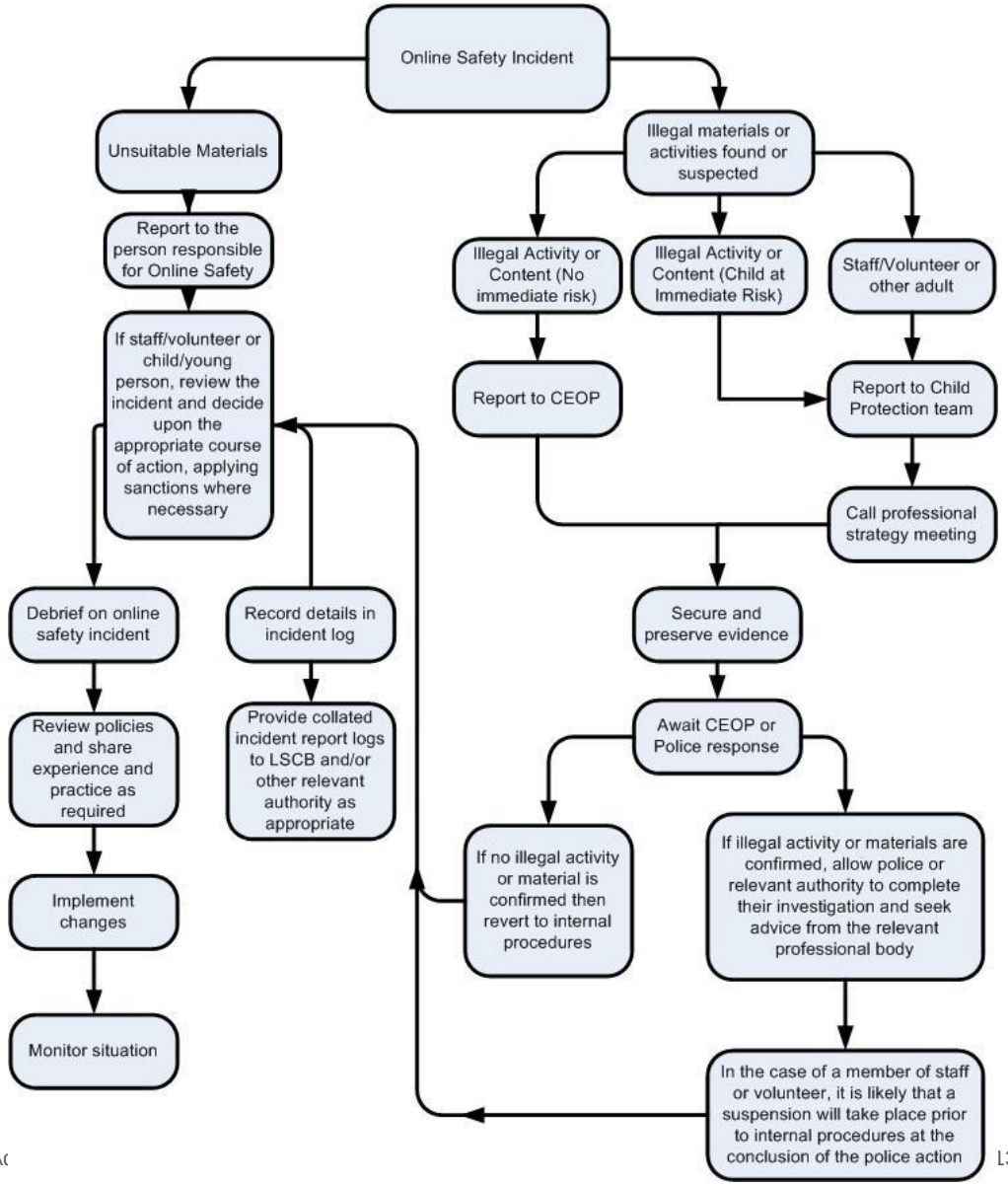
On-line gaming (educational)		X			
On-line gaming (non educational)		X			
On-line gambling				X	
On-line shopping / commerce			X		
File sharing			X		
Use of social media			X		
Use of messaging apps			X		
Use of video broadcasting eg Youtube			X		

Responding to incidents of misuse

This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities.

Illegal Incidents

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right hand side of the Flowchart for responding to online safety incidents and report immediately to the police.


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

Other Incidents

It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow the 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
    - 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 child protection purposes. The completed form should be retained by the group for evidence and reference purposes.

Sidney Stringer
Multi Academy Trust

E-Safety Policy
Specific School Policies:
Riverbank Academy

Academy Actions & Sanctions

Students

It is more likely that the schools 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/child protection procedures.

Incidents which are likely to be deemed as inappropriate include:

• **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 mobile device • Attempting to access or accessing the school / academy network, using another student's / pupil's account • Attempting to access or accessing the school / academy network, using the account of a member of staff • Corrupting or destroying the data of other users **DSL/Deputy DSL must be informed if students have been**: • Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature • Using proxy sites or other means to subvert the school's / academy'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	**Sanctions for misuse will be applied in line with our behaviour policy**

Staff

Actions / Sanctions

Incidents:	Refer to line manager	Refer to Headteacher	Refer to Local Authority / HR	Refer to Police	Refer to Technical Support Staff for action re filtering etc.	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable/inappropriate activites)		X	X	X				
Inappropriate personal use of the internet/social media /personal email	x	X			X	X		
Unauthorised downloading or uploading of files	X	X			X	X		
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	X	X			X	X		
Careless use of personal data e.g. holding or transferring data in an insecure manner	X	X				X		

Deliberate actions to breach data protection or network security rules		X			X			X
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		X	X	X	X			X
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature		X			X	X	X	X
Using personal email/social networking/instant messaging/text messaging to carry out digital communications with students		X				X	X	X
Actions which could compromise the staff member's professional standing	X	X				X	X	X
Actions which could bring the school/academy into disrepute or breach the integrity of the ethos of the school/academy		X				X	X	X
Using proxy sites or other means to subvert the school's /academy's filtering system	X				X	X		
Accidentally accessing offensive or pornographic material and failing to report the incident	X	X				X		
Deliberately accessing or trying to access offensive or pornographic material		X	X	X			X	X
Breaching copyright or licensing regulations	X	X			X	X		
Continued infringements of the above, following previous warnings or sanctions	X	X	X	X	X		X	X

Bring Your Own Device (BYOD) and 1:1 ownership

The educational opportunities offered by mobile technologies are being expanded as a wide range of devices, software and online services become available for teaching and learning, within and beyond the classroom. There are a number of e-safety considerations for BYOD that need to be reviewed to ensure that BYOD does not introduce vulnerabilities into existing secure environments. Considerations will need to include; levels of secure access, filtering, data protection, storage and transfer of data, mobile device management systems, training, support, acceptable use, auditing and monitoring.

- Students are permitted to bring their own devices into Academies and these should be connected to Wi-Fi on a system which allows users to authenticate themselves from a personal account and for monitoring of their internet use to be tracked to that username.
- The school has a set of clear expectations and responsibilities for all users
- The school adheres to the Data Protection Act principles
- All staff and parents/carers are provided with and accept the Acceptable Use Agreement (students where appropriate)
- All network systems are secure and access for users is differentiated
- Where possible these devices will be covered by the school's/academies normal filtering systems, while being used on the premises
- All users will use their username and password and keep this safe
- Mandatory training is undertaken for all staff
- Students/Pupils receive training and guidance on the use of personal devices
- Regular audits and monitoring of usage will take place to ensure compliance
- Any device loss, theft, change of ownership of the device will be reported to the e-learning lead or Headteacher

Staff Communication and Device Usage Policy (clarify this is personal phones not school ones)

	Staff & other adults		
Communication Technologies	Status		
Mobile phones may be brought to school	Allowed		
Use of mobile phones in lessons	Not allowed		
Use of mobile phones in social time	Allowed		
Taking photos on mobile phones / cameras	Not allowed		
Use of other mobile devices e.g. tablets, gaming devices	Not allowed		
Use of personal email addresses in school, or on school network	Allowed		
Use of school email for personal emails	Not allowed		
Use of messaging apps	Not allowed		
Use of social media	Not allowed		
Use of blogs	Not allowed		

Student Communication and Device Usage Policy

	Students				
Communication Technologies	Acceptable	Acceptable at certain times	Acceptable under staff supervision	Unacceptable	Unacceptable
Mobile phones may be brought to school	x				
Use of mobile phones in lessons		x	x		
Use of mobile phones in social time		X			
Taking photos on mobile phones / cameras				X	
Use of other mobile devices e.g. tablets, gaming devices		x			
Use of personal email addresses in school, or on school network		X			
Use of school email for personal emails				x	
Use of messaging apps				X	
Use of social media				X	
Use of blogs			X		

Key information shared and adopted by all staff at Riverbank Academy:

- If staff must use USB's you must make ensure **they are encrypted**
- Any visitors to schools should use guest passes

Username	Password
guest1	**Tallon1**
guest2	**Tallon2**

- Do not accept friend requests from students (think carefully before accepting former students requests)
- School email is allowed on **personal devices*** as long as the device is password protected
- School photos and videos are not allowed on **personal devices**
- Videos and photos of students are allowed on **devices purchased by the school** and managed centrally by our MAT IT team
- **School devices can be used at home for work purposes**. They must not be shared with anyone that is not employed by the academy and must be password protected.