

# Online Safety Policy

## Riverbank Academy

Adopted and Adapted from The Sidney  
Stringer Multi Academy Trust

## E-Safety Policy

Sidney Stringer Multi Academy Trust

**Approved by:**  
**Date:** May 2025  
**Reviewed by:** Andrew Walls  
**Next review due by:** May 2026

# Development of this Policy

This e-safety policy has been developed by the SSA MAT safeguarding group consisting of Headteachers, safeguarding leads, ICT network and curriculum leads, along with Governor, staff and student representation. Consideration has been given to current legislation, including Keeping Children Safe in Education (KCSIE), UK GDPR, and guidance on emerging online risks including Artificial Intelligence. This policy explicitly aligns with and complements the Sidney Stringer Multi Academy Trust's AI Policy, ensuring a cohesive approach to digital technologies.

Consultation with the whole school community, including specific focus groups on digital citizenship and the ethical use of AI, has taken place through a range of formal and informal meetings.

Schedule for Review:

|                                                                                                                                                                                                                                                                                                                                                      |                                                                                                                                                                                      |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| The implementation of this e-safety policy will be monitored by the:                                                                                                                                                                                                                                                                                 | Vice Principal (MAT) - Sustainability, Data, Assessment and IT (with responsibility for e-safety).                                                                                   |
| Monitoring will take place at regular intervals:                                                                                                                                                                                                                                                                                                     | Annually (or more frequently if significant new threats or technologies, including rapid AI developments, emerge).                                                                   |
| 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 and trends, including near misses, concerns related to digital wellbeing, and incidents involving AI misuse) 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 (e.g., AI-generated deepfakes, advanced phishing, online radicalisation, misuse of AI tools) or incidents that have taken place. The next anticipated review date will be: | May 2026                                                                                                                                                                             |
| Should serious e-safety incidents take place, the following external persons / agencies should be informed:                                                                                                                                                                                                                                          | Please refer to flow chart at end of document (and local safeguarding partnership procedures, ensuring alignment with reporting requirements for AI-related harms where applicable). |

The school will monitor the impact of the policy using:

- Logs of reported incidents
- Monitoring logs of activity (including sites visited and application usage, including approved AI tools, where appropriate and lawful)
- Internal monitoring data for network activity and security alerts
- Surveys / questionnaires of:
  - students / pupils (including questions on digital citizenship, wellbeing, and their understanding and use of AI)
  - parents / carers
  - staff
- Feedback from student digital leaders/ambassadors.
- Analysis of pastoral care records related to online issues.
- Review of Data Protection Impact Assessments (DPIAs) conducted for new technologies, particularly AI tools.

## 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, digital learning environments, approved Artificial Intelligence (AI) tools, and associated online services, both in and out of the Academies/Schools. This includes the use of personal devices for school-related activities (BYOD) where permitted and the use of AI on such devices for educational purposes.

Each academy will deal with such incidents within this policy and associated behaviour and acceptable use policies (AUPs), which include guidelines for AI usage. They will, where known, inform parents/carers of incidents of inappropriate e-safety behaviour that take place outside of the school environment if it impacts the individual or school community. Each school/academy will report these incidents back to the MAT Safeguarding Committee.

## Roles and Responsibilities

### Governors:

Governors in each Academy with safeguarding responsibility are responsible for the approval of the E-Safety Policy and ensuring its alignment with the MAT AI Policy. They are responsible for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about e-safety incidents, trends, training compliance, DPIA summaries for AI tools, and monitoring

reports.

Safeguarding Governors for each Academy should:

- regularly attend at the MAT safeguarding committee
- regularly monitor e-safety incident logs and ensure actions are appropriate and timely, including those related to AI
- Champion a culture of e-safety, digital citizenship, and responsible AI use across the Academy.

Adapted from template provided by SWGfL - AW © All rights reserved SWGfL 2013

- 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 and digital wellbeing, and promoting the ethical use of AI) 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 and KCSIE guidance). They must also ensure adherence to the MAT AI Policy, particularly regarding human oversight and accountability.
- The Headteacher/Principal/Senior Leaders are responsible for ensuring that the E-Safety Coordinator/Officer and other relevant staff receive suitable and regularly updated training to enable them to carry out their e-safety roles and to train other colleagues, as relevant. This includes training on new and emerging risks, such as those posed by AI, and the principles outlined in the MAT AI Policy.

### **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. This role includes overseeing the e-safety aspects of AI use.

- attends the MAT Safeguarding Committee meetings to report any e-safety incidents
- ensures regular review of network security logs, filtering reports, and other relevant monitoring data, including logs from AI systems where appropriate and feasible.
- 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 in line with MAT guidance and the MAT AI Policy

- 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, students, and parents/carers on e-safety matters, including digital citizenship, responsible AI use, understanding AI limitations, and identifying AI-generated misinformation, in line with the Core Principles of the MAT AI Policy.
- liaise with the Headteacher who will decide whether to contact a relevant authority
- liaises with school technical staff and the MAT Network Manager, particularly regarding the secure implementation and monitoring of AI tools.
- receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments and risk assessments.
- Promotes a positive culture of digital citizenship, critical thinking online, and student agency in the use of digital technologies, including AI.
- Supports the process of conducting DPIAs for AI tools.

### **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, including regular vulnerability assessments and penetration testing where appropriate. This includes securing systems that host or interact with AI tools.
- that the academy meets required internal e-safety technical requirements, data protection standards for AI systems, and any relevant national standards or Local Authority Guidance that may apply.
- that users may only access the networks, cloud managed systems, and approved AI tools audited and operated by the Academy and devices through a properly enforced password protection policy and multi-factor authentication (MFA) where appropriate, especially for staff and sensitive systems.
- that they keep up to date with e-safety technical information and emerging cyber threats, including those targeting AI systems, in order to effectively carry out their e-safety role and to inform and update others as relevant
- that the use of the network and approved AI tools 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 12 characters in length, incorporating complexity requirements, and that users are prompted for regular password changes. Passphrases are encouraged.

### **Teaching and Support Staff**

are responsible for ensuring that:

- they have an up to date awareness of e-safety matters, digital citizenship principles, the potential risks and benefits of emerging technologies like AI (as outlined in the MAT AI Policy), and of the current academy e-safety policy and practices
- they have read, understood and signed the Staff Acceptable Use Policy (AUP) annually, which includes guidelines on AI use.
- they report any suspected misuse or problem to the E-Safety Officer for investigation, including concerns about AI-generated content or unethical AI use.
- all school digital communications with students/pupils/parents/carers should adhere to the MAT staff code of conduct and professional boundaries
- 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, sexting, cyberbullying, misinformation/disinformation (including AI-generated), online radicalisation, and responsible AI use (including data privacy, bias awareness, and academic integrity).
- students understand and follow the e-safety and acceptable use policies, including guidelines for AI.
- students have a good understanding of research skills, critical evaluation of online sources (including AI-generated content, as per the AI Policy's emphasis on Student Agency and Digital Literacy), and the need to avoid plagiarism and uphold copyright regulations
- they monitor the use of digital technologies, mobile devices, cameras, and AI tools etc. in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- in lessons where internet use or AI tool use is pre-planned students should be guided to approved sites and tools checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches or via AI tools. Human oversight is maintained as per the AI Policy.
- They model positive digital citizenship and support students in developing digital resilience, wellbeing strategies, and a critical understanding of AI and its implications.
- They adhere to the pedagogical principles for AI use as outlined in the MAT AI Policy, ensuring AI supports and augments teaching, rather than replacing educator roles.

### **Child Protection Officer (Designated Safeguarding Lead - DSL)**

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 (including via AI tools)
- access to illegal / inappropriate materials
- inappropriate on-line contact with adults / strangers

- potential or actual incidents of grooming
- cyber-bullying
- Online radicalisation and exposure to extremist ideologies.
- Harmful AI-generated content (e.g., deepfakes used for bullying or non-consensual image generation).
- Impacts on mental health and wellbeing from online activities, including pressures related to AI.
- Understanding how AI might be used in safeguarding contexts (e.g., monitoring tools) and the associated ethical considerations, as per the AI Policy (5.4 AI for Safeguarding).

## Students:

- are responsible for using the academy digital technology systems, online resources, and approved AI tools in accordance with their understanding of the Student Acceptable Use Policy, principles of good digital citizenship, and guidelines for ethical AI use.
- have a good understanding of research skills, critical evaluation of online information (including AI-generated content, promoting student agency as per the AI Policy), and the need to avoid plagiarism and uphold copyright regulations when using any resource, including AI.
- need to understand the importance of reporting abuse, misuse, access to inappropriate materials, or anything online (including from AI interactions) that makes them feel uncomfortable or unsafe, 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 or if it brings the school into disrepute, for their age and ability.
- Understand the ethical implications of using AI tools, the importance of academic integrity, and the potential for bias in AI outputs. They will be taught not to share personal data with public AI tools unless explicitly part of an approved, secure educational activity.
- Are encouraged to be positive digital citizens, respectful of others online, mindful of their digital footprint, and to use AI responsibly.

## Parents/Carers

Parents/Carers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices and other digital technologies, including AI tools, in an appropriate and safe way. The academies will take every opportunity to help parents understand these issues through parents'

evenings, newsletters, letters, website, social media channels, and information about national / local e-safety campaigns / literature and resources (e.g., guidance on parental controls, online safety settings, conversation starters about online life, and the school's approach to AI in education as per the AI Policy). 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, Chromebooks, and other personal devices.
- Discussing online safety, digital wellbeing, and responsible AI use regularly with their children.

## Community Users

Community Users who access school systems, networks, or approved AI tools as part of the wider academy provision will be expected to sign a Community User AUP before being provided with access to school systems.

## 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 and develop critical thinking skills, especially in relation to AI. The education of students in e-safety and digital citizenship (including AI literacy) 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 (including those associated with AI) and build their resilience and digital wellbeing.

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 and digital citizenship curriculum should be provided as part of the tutorial programme, assemblies, PSHE, and the computing curriculum along with other lessons and should be regularly revisited and adapted to reflect current trends and risks, including the ethical use and implications of AI, as promoted by the AI Policy (Student Agency and Digital Literacy).
- Students will be taught to approach the appropriate authority in each school regarding any e-safety concerns and to report when they are concerned, effected or unsettled by a form of concerning electronic conduct, contact or content, including online bullying, grooming, or exposure to harmful material, misinformation, or problematic AI-generated content.
- E-Safety and Digital Citizenship, including AI literacy, forms part of the scheme of work for IT and

Computer Science teaching at all Academies.

- In Secondary Academies the tutorial programme will have a commitment to delivering a series of lessons focusing on e-safety each year. These should ideally be **run** around, and in line, with the themes covered in Safer Internet Day **and other relevant awareness campaigns, incorporating AI safety messages.**
- Students should be taught in lessons to be critically aware of the materials/content they access on-line, **including that generated by AI (as per AI Policy principles on Transparency and Student Agency),** and be guided to validate the accuracy of information **and identify potential biases.**
- Students should be taught to acknowledge the source of information used, **understand intellectual property, cite AI assistance appropriately where permitted,** 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, **mobile devices, and AI tools.**
- In lessons where internet use **or use of approved AI tools** is pre-planned, it is best practice that students should be guided to **approved sites and tools** checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches **or through AI interactions.**
- Where students are allowed to freely search the internet **or use approved AI tools,** staff should be vigilant in monitoring the content **accessed or generated by** the young people **visit/use, ensuring human oversight.**
- It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs, discrimination, **controversial historical events**) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff can temporarily **adjust filtering for specific, supervised activities.** Any request to do so, should be auditable, with clear reasons for the need **and a defined timeframe.** **Similar considerations apply to access to specific AI functionalities if usually restricted.**

## **Education - parents/carers**

Many parents and carers have **varying levels of understanding** of e-safety risks and issues, **including those related to AI,** 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, **face social pressures online, or engage with AI without full understanding,** 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 and information evenings (including specific sessions on AI in education)
- Letters, newsletters, website and social media updates, including information about the MAT AI Policy and its implications.
- Parents/Carers evenings specifically focused on online safety, digital wellbeing, and the responsible use of AI.
- High profile events / campaigns e.g. Safer Internet Day
- Reference to the relevant web sites / publications e.g. [www.swgfl.org.uk](http://www.swgfl.org.uk) [www.saferinternet.org.uk/](http://www.saferinternet.org.uk/) <http://www.childnet.com/parents-and-carers> [www.nspcc.org.uk/keeping-children-safe/online-safety/](http://www.nspcc.org.uk/keeping-children-safe/online-safety/) and [thinkuknow.co.uk](http://thinkuknow.co.uk)
- Guidance on using parental controls, privacy settings on devices and platforms, and discussing ethical AI use with their children.

## 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:

Adapted from template provided by SWGfL - AW © All rights reserved SWGfL 2013

- Providing family learning events in the use of new digital technologies, digital literacy, AI awareness (benefits, risks, ethical considerations), and e-safety.
- The school / academy website will provide e-safety information and resources, including links to the MAT AI Policy, for the wider community.

## Education & Training – Staff / Volunteers

It is essential that all staff receive regular and relevant e-safety training and understand their responsibilities, as outlined in this policy and the MAT AI 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 to cover new threats, technologies (including AI developments, data protection implications of AI, pedagogical uses of AI, and identifying AI-generated misinformation or bias, as per AI Policy section 3 & 5), and changes in legislation/guidance. 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, Acceptable Use Agreements, their role in safeguarding pupils online, and the key principles of the MAT AI Policy regarding responsible AI use.
- 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 with appropriate restrictions 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, including on the safe and ethical use of specific AI tools.

## 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 or MAT-provided governor training, which will include oversight responsibilities related to the MAT AI Policy.

## 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, including those supporting AI tools, will be managed in ways that ensure that the schools meet recommended technical requirements and industry best practices for security and data protection. DPIAs will be conducted for AI tools processing personal data, as mandated by the AI Policy.
- There will be regular reviews and audits of the safety and security of each school's 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, devices, and AI tools, based on the principle of least privilege.
- 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. Multi-Factor Authentication (MFA) will be implemented for staff access to key systems.
- Access to administrator credentials for MAT ICT systems used by the Network Manager (or other person) must be managed securely, with break-glass procedures in place for emergency access by authorised personnel like the Headteacher/Principal, and all such access logged and audited.
- The MAT ICT Network Manager is responsible for ensuring that software licence logs, including for AI tools, 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.

Adapted from template provided by SWGfL - AW © All rights reserved SWGfL 2013

- 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. Filtering will be appropriate to the age and maturity of users and will aim to block access to harmful and inappropriate content, including pornography, violence, sites promoting radicalisation or discrimination, and known malicious AI-driven sites. Filtering levels will be regularly reviewed.
- There is a clear process in place to deal with requests for filtering changes, including access to specific AI tools or platforms. 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 or AI tool is purely educational and aligns with the MAT AI Policy and should be unblocked/approved. This will be forwarded to Trust IT Support to unblock within a reasonable timeframe (e.g., 24-48 hour window).
  - Category Two: The website or AI tool is educational but may pose a low level of risk (e.g., data privacy concerns with an AI tool, mature themes on a website). 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 (including a DPIA for AI tools as per AI Policy) 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/tool. This will then be carried out by the MAT IT Support Staff.
  - Category Three: The website or AI tool would involve a serious change to the use of internet access or data processing 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 or AI tool 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 MAT Safeguarding Meeting and by the DPO if significant personal data is involved. This includes requests for access to new AI tools or platforms not previously vetted.
- 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, including usage of approved AI tools where feasible and appropriate, 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 **at least annually** with reports issued to the MAT Vice Principal with Responsibility for E-Safety. The school infrastructure and individual workstations are protected by up to date **endpoint detection and response (EDR) or** 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 **regularly (e.g., monthly or termly)**.
- 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. **These devices must be encrypted and password protected.**
- 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, **approved AI tools that require local installation**). 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, **and be subject to a risk assessment and DPIA where necessary, in line with the AI Policy. Users must not input sensitive personal data into unapproved AI tools.**
- The Academy officially supports data being stored in Academy managed and audited cloud based storage systems **(e.g. Google Workspace)**, 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) **in compliance with UK GDPR and the principles of data minimisation stated in the AI Policy, especially when AI tools might process this data. Data used to train enterprise-level AI models must be handled according to contractual agreements ensuring it is not used improperly by third parties.**

- The use of portable USB storage devices (USB sticks, external hard drives) is strongly discouraged and should only be used in exceptional circumstances with encryption and explicit permission from the Vice Principal for MAT IT. Data should preferably be stored on either servers owned by the Multi Academy Trust or cloud services that are managed by the Multi Academy Trust. Individual academies will still be able to record images directly to portable storage inside digital cameras but these should be transferred to an academy audited system and deleted from the portable storage on the same day that they are taken.
- Students are not permitted to use USBs and should be directed to cloud based storage systems as their primary means of portable storage. Any exceptions must be approved by the Vice Principal for MAT IT for specific tasks and data transfer must be supervised by a member of MAT IT Support.

## Use of digital and video images and AI-generated media

The development of digital imaging and AI media generation technologies has created significant benefits to learning, allowing staff and students/pupils instant use of images that they have recorded themselves, generated using approved AI tools, or downloaded from the internet. However, staff, parents/carers and students/pupils need to be aware of the risks associated with publishing digital images or AI-generated media (especially those depicting individuals) on the internet. Such images or media may provide avenues for cyberbullying or misrepresentation (e.g. deepfakes, non-consensual image alteration) to take place. Digital images and media 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 or AI-generated media, staff should inform and educate students about the risks associated with the taking, use, sharing, publication and distribution of such media, including ethical considerations around AI image generation, consent, and potential for misuse (e.g. creating deepfakes). In particular they should recognise the risks attached to publishing their own images or likeness 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. Parents/carers must not take photos or videos of other children without explicit consent from those children's parents/carers. The creation or sharing of AI-generated images of other students by parents is not permitted.
- Staff and volunteers are allowed to take digital/video images or use approved AI tools to generate educational media (in line with the AI Policy's pedagogical focus) to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images/media. Those images or media outputs should only be taken or generated on school equipment or approved platforms; the personal equipment of staff should not be used for such purposes unless explicitly authorised and risk assessed (e.g. for a school trip where school devices are impractical, with immediate secure transfer and deletion from personal device) and stored to a school monitored and audited storage system (the school network or Google Workspace).
- 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. Consent must be obtained before using student images or likenesses in AI-generated media, and

the output reviewed for appropriateness and bias by a human before use.

- Students must not take, use, share, publish or distribute images or AI-generated likenesses (e.g. deepfakes) of others without their permission.
- Photographs and other media, including AI-generated visuals featuring students, 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 and media, ensuring appropriate consents are in place and transparency about AI use if applicable.
- Students' full names will not be used anywhere on a website or blog, particularly in association with photographs, unless explicit consent is given for specific, limited purposes (e.g., celebrating achievements).
- Written permission from parents or carers will be obtained before photographs or AI-generated media featuring identifiable students are published on the school website (list to be compiled from Parent/Carer AUP at the start of each year). This consent will clearly state how and where images/media will be used, for how long, and if AI was involved in its creation.
- Student's work can only be published with the permission of the student and parents or carers. If AI tools were used in creating the work, this should be appropriately acknowledged where relevant.

## Data Protection

Please refer to the MAT Data Protection Policy which outlines the position of the Sidney Stringer Multi-Academy Trust on Data Protection. This E-Safety Policy also incorporates the data protection principles specific to AI use as detailed in the MAT AI Policy (Section 4).

Personal data will be recorded, processed, transferred and made available according to the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018, which states that personal data must be:

- Fairly and lawfully processed and in a transparent manner
- Processed for specified, explicit and limited purposes
- Adequate, relevant and not excessive (data minimisation, especially important for data fed into AI systems)
- Accurate and, where necessary, kept up to date
- Kept no longer than is necessary (storage limitation, with clear retention schedules for data used by AI tools)
- Processed in accordance with the data subject's rights
- Secure (integrity and confidentiality, with robust security for AI systems and data)
- Only transferred to others with adequate protection. (Particular scrutiny for third-party AI providers as per AI Policy 4.1).

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. This applies to data processed by AI tools.
- 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". Privacy notices will be updated to include information about the use of AI tools processing personal data, as per AI Policy 4.3.
- It has a Data Protection Policy and associated procedures which are regularly reviewed, including DPIA procedures for AI systems.
- It is registered as a Data Controller with the Information Commissioner's Office (ICO) for the purposes of the UK General Data Protection Regulation.

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. This includes adhering to clear desk and clear screen policies, and not inputting identifiable personal data into public/unapproved AI tools.
- Use personal data only on secure password protected computers and other devices, utilising

multi-factor authentication where available, 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. Avoid using unsecure personal email or messaging apps for transferring personal data. All data transfers to third-party AI providers must be secure (AI Policy 4.4).

## Communications

A wide range of rapidly developing communications technologies, including AI-powered communication tools, has the potential to enhance learning. The MAT encourages the safe and responsible use of these technologies, guided by the Core Principles of the AI Policy. 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 and other approved communication platforms (e.g., secure VLE messaging, school communication apps, approved AI chatbots for specific functions) may be regarded as safe and secure and are monitored. Users should be aware that official digital communications are monitored for safeguarding and compliance purposes, with transparency about AI involvement in communication if applicable.
- Users must immediately report, to the nominated person - in accordance with the MAT policy, the receipt of any communication (including from AI systems) 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 or approved platform. 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 or approved school platforms 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 and maintaining appropriate digital boundaries, including when interacting with AI. 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 of students or staff (beyond designated professional contact details) should not be posted on the academy website and only official email addresses or approved communication channels should be used to identify members of staff.

## Social Media - Protecting Professional Identity and Maintaining Boundaries (including AI use)

Expectations for teachers' professional conduct are set out in 'Teachers Standards (updated versions as applicable) and Keeping Children Safe in Education'. Ofsted's e-safety framework (and subsequent guidance) 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 privacy settings; data protection; reporting issues. Clear reporting guidance, including responsibilities, procedures and sanctions. Guidance on maintaining professional boundaries online, and the professional implications of personal AI use.
- Risk assessment, including legal and reputational risk.

School staff should ensure that:

- No reference should be made in social media to students, parents/carers or school staff in a way that could identify them or breach confidentiality, or bring the school into disrepute.
- They do not engage in online discussion on personal matters relating to members of the school community that could undermine professional relationships or trust.
- Personal opinions expressed online, particularly on controversial topics, or outputs from personal use of AI tools, should not be attributed to their school or the MAT and should not compromise their professional standing.
- Security and privacy settings on personal social media profiles are regularly checked to minimise risk of loss of personal information and unintended exposure.
- They do not accept friend requests or follow requests from current students on personal social media accounts. Communication should be via official channels.
- They consider the long-term implications of their online conduct and digital footprint, including content generated or shared using AI, on their professional reputation.
- They use AI tools for professional purposes in line with the MAT AI Policy, ensuring data protection and ethical considerations are met, and do not use personal student data in public AI tools.

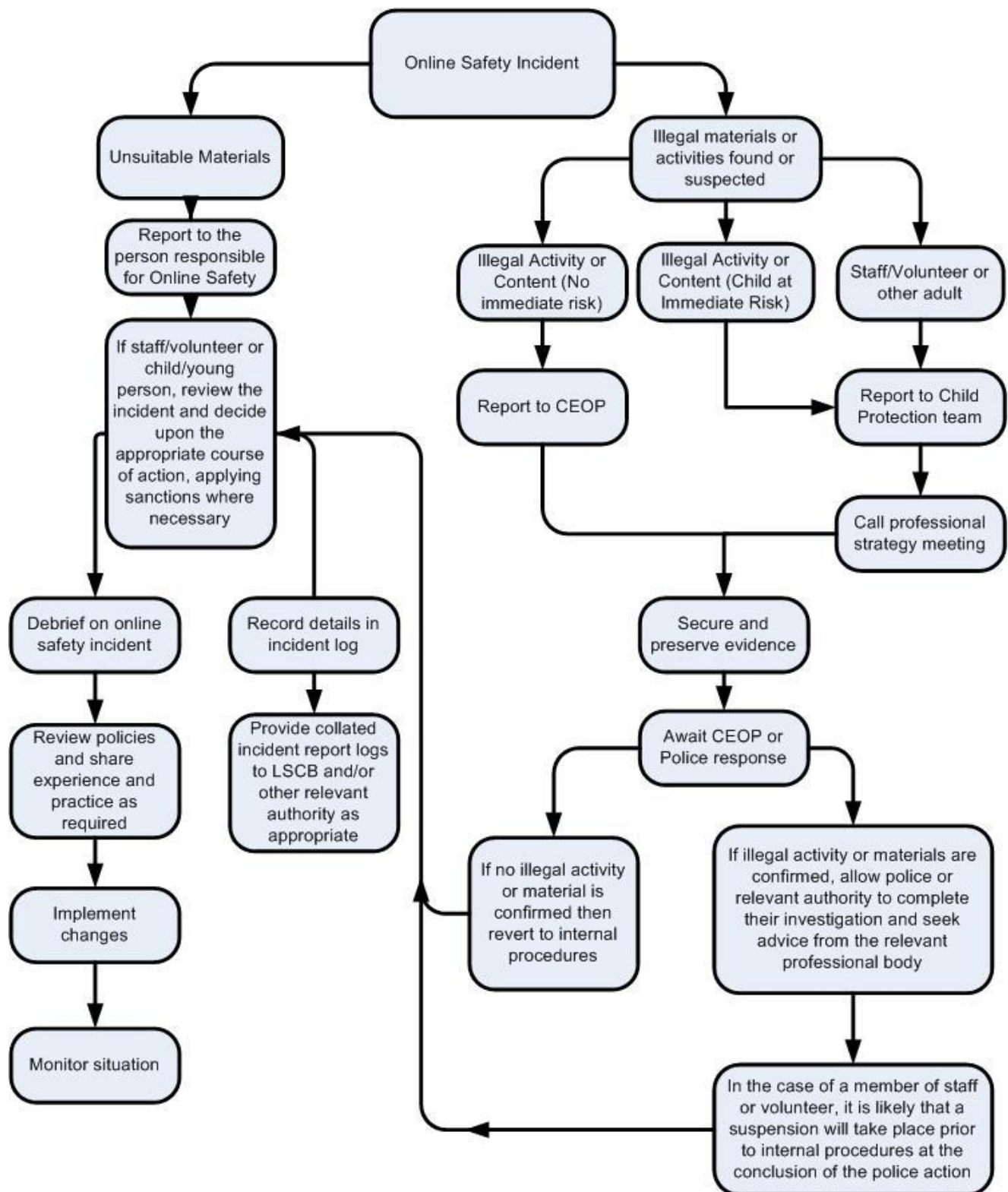
## Other Incidents

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.



## Responding to incidents of misuse - Flow Chart

### 3.5 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 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                          |            |                             |                                |              | 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 |  |  |

## 4.0 School/Academy Actions & Sanctions

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 procedures as follows:

### 4.1 Student/Pupils Actions/Sanctions

| Note - it is permitted for the Assistant Principal for MAT ICT to check the security of these systems and to attempt to circumvent and carry out the below as part of security/penetration testing. This will be done with advanced warning to the headteacher of each Academy and the Executive Principal. | Refer to class teacher / tutor | Refer to Pastoral Leader | Refer to Headteacher / Principal | 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 intervention sanction eg detention / exclusion |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------|--------------------------|----------------------------------|-----------------|--------------------------------------------------------------------------|-------------------------|---------------------------------------------|---------|--------------------------------------------------------|
| <b>Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).</b>                                                                                                                                         |                                | X                        | X                                | X               | X                                                                        | X                       |                                             |         |                                                        |
| Unauthorised use of non-educational sites during lessons                                                                                                                                                                                                                                                    | X                              | X                        |                                  |                 |                                                                          |                         |                                             |         | X                                                      |
| Unauthorised use of mobile phone / digital camera / other mobile device                                                                                                                                                                                                                                     | X                              | X                        |                                  |                 |                                                                          |                         |                                             |         | X                                                      |
| Unauthorised use of social media / messaging apps / personal email                                                                                                                                                                                                                                          | X                              | X                        |                                  |                 |                                                                          |                         |                                             |         | X                                                      |
| Unauthorised downloading or uploading of files                                                                                                                                                                                                                                                              | X                              | X                        |                                  |                 | X                                                                        |                         |                                             |         | X                                                      |
| Allowing others to access school / academy network by sharing username and passwords                                                                                                                                                                                                                        |                                | X                        |                                  |                 | X                                                                        | X                       |                                             |         | X                                                      |
| Attempting to access or accessing the school / academy network, using another student's / pupil's account                                                                                                                                                                                                   |                                | X                        |                                  |                 | X                                                                        | X                       |                                             |         | X                                                      |
| Attempting to access or accessing the school / academy network, using the account of a member of staff                                                                                                                                                                                                      |                                | X                        | X                                |                 | X                                                                        | X                       |                                             |         | X                                                      |
| Corrupting or destroying the data of other users                                                                                                                                                                                                                                                            |                                | X                        | X                                |                 |                                                                          | X                       |                                             |         | X                                                      |
| Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature                                                                                                                                                                                                         |                                | X                        | X                                |                 |                                                                          | X                       |                                             |         | X                                                      |
| Continued infringements of the above, following previous warnings or sanctions                                                                                                                                                                                                                              |                                |                          | X                                |                 |                                                                          | X                       | X                                           |         | X                                                      |
| Actions which could bring the school into disrepute or breach the integrity of the ethos of the school                                                                                                                                                                                                      |                                | 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 |   |  |   |
| Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act | X | X |   |   |   |   | X |  | X |

## 4.2 Staff Actions/Sanctions

| Incidents:                                                                                                                                                          | Refer to line manager | Refer to Headteacher Principal | Refer to Local Authority / HR | Refer to Police | Refer to Technical Support Staff for action re filtering etc. | Warning | Suspension | Disciplinary action |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|--------------------------------|-------------------------------|-----------------|---------------------------------------------------------------|---------|------------|---------------------|
| <b>Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).</b> |                       | 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 |

## 4.3 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 principles of the General Data Protection Regulation
- All users are provided with and accept the Acceptable Use Agreement
- 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

## 4.4 Staff and other Adults Communication and Device Usage Policy

| Communication Technologies                               | Allowed | Allowed at certain times | Allowed for selected staff |
|----------------------------------------------------------|---------|--------------------------|----------------------------|
| Mobile phones may be brought to school                   | X       |                          |                            |
| Use of mobile phones in lessons                          |         | 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 |   |  |

## 4.5 Student Communication and Device Usage Policy

|                                                                 | Acceptable | Acceptable at certain times | Acceptable under staff supervision | Unacceptable |
|-----------------------------------------------------------------|------------|-----------------------------|------------------------------------|--------------|
| Communication Technologies                                      |            |                             |                                    |              |
| Mobile phones may be brought to school                          |            | X                           |                                    |              |
| Use of mobile phones in lessons                                 |            |                             |                                    | 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                                  |              |

# Student / Pupil Acceptable Use Policy Agreement

This is how we stay safe when we use computers:

- I will ask a teacher or suitable adult if I want to use the computers / tablets

- I will only use activities that a teacher or suitable adult has told or allowed me to use

- I will take care of the computer & other equipment.

- I know that if I break the rules I might not be allowed to use a computer / tablet

- I will respect others when online and think about what I say

• 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

• I will tell a teacher or suitable adult if I see something that

upsets me on the screen

Signed

Date