E SAFETY POLICY

Development and review of this Policy

This e-safety policy has been developed by the named 'Persons Responsible' below in conjunction with the Trust Director of Technology, discussed with senior leaders and approved by the Board of Trustees.

Should serious e-safety incidents take place one of the following people should be contacted:	***FOR SOUTHMOOR ACADEMY*** *Olivia Thompson - Lead Designated Person* *Nicola Doherty - Designated Person* *In the case where none of the above are available, the following may be contacted:* *Joanne Maw - Headteacher*	***FOR SANDHILL VIEW ACADEMY*** *Allison Johnston – Lead Designated Person* *Amy O'Donnell – Designated Person* *In the case where neither of the above are available the following may be contacted:* *Jill Dodd – Headteacher*
For education opportunities for children:	***AT SOUTHMOOR ACADEMY*** *Simon Wareham – Assistant Head* *In cases where the above are not available:* *Contact Business Computing Department.*	***AT SANDHILL VIEW ACADEMY*** *Anthony Blake – Assistant Head* *In cases where the above are not available:* *Contact ICT Department.*
To report concerns about network infrastructure or available content:	***AT SOUTHMOOR ACADEMY*** *Tom Malone - Trust Director of Technology* *In the case where none of the above are available the following may be contacted:* *Joanne Maw – Headteacher* *Sammy Wright – Head of School*	***AT SANDHILL VIEW ACADEMY*** *Tom Malone – Trust Director of Technology* *In the case where none of the above are available the following may be contacted:* *Jill Dodd – Headteacher* *Allison Johnston - Deputy Head*

Further monitoring of the policy will take place by the monitoring of:

- Reported incidents in school
- Logs of questionable internet and network activity
- Surveys/Questionnaires of students, teachers/staff, parents, carers when appropriate

Person responsible: Tom Malone (Trust Director of Technology)
Allison Johnston (Deputy Head/DSL – Sandhill View Academy)
Olivia Thompson (Assistant Head/DSL – Southmoor Academy)

Last review date: 13.03.24

Scope of the Policy

All stakeholders at Aspire North East Multi Academy Trust are expected to adhere to this policy including staff, students, volunteers, parents, carers, visitors, community members and any other person who may use Trust ICT. This policy extends to the ICT used within academies in the Trust and any ICT and ICT platforms provided by the Trust that may be used within or outside the Trust.

In accordance to the Education and Inspections Act 2006, the Headteacher is entitled to regulate the behaviour of students when they are both within and outside of school. The law empowers members of staff to issue relevant sanctions to students for inappropriate behaviour. This behaviour may include cyberbullying or other incidents covered by this policy or those not covered by the policy that may be deemed inappropriate by the Trust.

Furthermore, the 2011 Education Act extends the power of schools to search for and search the actual electronic devices and empowers schools to delete data as appropriate. The scope of the powers on our Trust is limited by those which we have identified as online issues in accordance with the Behaviour Policy.

The Trust will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known and when possible attempt to inform parents/carers of incidents of inappropriate e-safety behaviour that takes place out of school.

Roles and Responsibilities

The following stakeholders have responsibilities within the scope of this policy as detailed.

Trustees

Trustees are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. Trustees are also required to:

- Regularly hold those responsible for safeguarding to account in relation to e-safety
- Monitoring of e-safety incidents
- Keeping up to date with relevant changes within this area and holding each Academy to account

CEO, Headteacher and Senior Leaders:

- The CEO / Headteacher have a duty of care for ensuring the safety (including e-safety) of members of the Academy. They may delegate this responsibility as appropriate to relevant persons including those who are identified as designated persons.
- The CEO / Headteacher should arrange relevant procedures that should be followed in the event of a serious e-safety allegation being made against a member of staff.
- The CEO / Headteacher / Senior Leaders are responsible for ensuring that relevant members of the Trust community are trained within e-safety.
- The CEO / Headteacher / Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal e-safety monitoring role.
- The Senior Leadership Team will receive regular monitoring reports and communication from designated persons investigating any breach of acceptable standards of e-behaviour.

Designated persons:

- May be requested to lead on any e-safety investigations when appropriate.
- Takes day-to-day responsibility for e-safety issues and has a leading role in establishing and reviewing the Trust E-safety policies with the Assistant Head (Southmoor) / Deputy Head (Sandhill View)
- Ensures that all staff know what to do when there has been a serious breach of e-safety.

- Provides training and advice for staff when appropriate including members of staff who are new to the Trust community.
- Liaises with relevant external third parties on behalf of the Trust.
- Liaises with Trust technical staff.
- Receives reports of e-safety incidents and works with the relevant Assistant Head with responsibility to inform the curriculum delivered within Personal Development.
- Meets with relevant members of the Board of Trustees / Academy Council that have responsibility for safeguarding and provides information as appropriate about e-safety incidents.
- Communicate efficiently with the Senior Leadership Team when deemed appropriate.
- Should be trained in e-safety issues and be aware of the potential safeguarding issues to arise from:
  - sharing of personal data.
  - access to illegal / inappropriate materials including photographs, videos and articles.
  - inappropriate on-line contact with adults / strangers and associated risks.
  - potential or actual incidents of grooming.
  - cyber-bullying.
  - radicalisation and extremism.

IT Department

The IT department must:

- Ensure that the Trust's technical infrastructure is secure and puts measures in place to prevent computer misuse and/or malicious attacks.
- Ensures that the Trust's network meets required e-safety technical requirements and that security measures put in place are appropriate for a school environment.
- Ensures that proper password protection and practice is implemented to uphold the security of the Trust network.
- Decides on relevant filtering and updates filtering when appropriate.
- Ensure 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.
- Ensure that the use of the network and peripheral services are regularly monitored in order to ensure that any attempted misuse can be.
- Ensure data can be recovered from backup without corruption in a timely fashion
- Ensure that all PC's have anti-virus on them
- Ensure the IT could infrastructure is secure
- Ensure the Cloud infrastructure is secure and backed up

Computing devices that belong to the Trust are not be given or loaned to students to then be removed from site without filtering and monitoring software installed on to them from the Trust IT department.

Computing devices that belong to the Trust that are given or loaned out to students to take away from the Trust must be named the same as the pupil and login name must be the same as the pupil.

Staff are not to remove computing devices from the school site with the purpose of letting a student use the device without filtering and monitoring software being installed in the first instance by the Trust IT department.

Any computing device that has gone outside the Trust at any point must be in a state that if and when it is returned, that the device is not a threat to the Trust network.

All computing devices are secured on the correct network within the Trust.

Any illegal activity on Trust computing devices or on the Trust network will result with the proper authorities being informed. Any attempt of illegal activity on Trust computing devices or on the Trust

network will result with the proper authorities being informed. Any attempt to circumvent the Trust network will result in the account being barred until SLT see fit to allow said person back on to the network.

Staff should take the following steps to ensure they are working within the cyber security guidelines:

General information

- 1. Review the privacy settings for your social media, professional networking site and app accounts.
- 2. Know who to report any unusual activity to. If you are unsure, ask your line manager or IT team.
- 3. Check your device is set to receive updates automatically.
- 4. Remove any apps that have not been downloaded from official stores.
- 5. For your most important accounts, set a strong password and switch on two-factor authentication, if available
- 6. Check that the password for your work account is unique.
- 7. If it's not possible to follow security advice – flag it to your IT team.
- 8. Lock your PC when you are away from it.

A Filtering and Monitoring Checklist must be completed every year by IT.

Teaching and Support Staff:

Including any other member of staff that may come into contact with students have a responsibility to ensure:

- They are aware of the e-safety policy and accepted practices within the Trust.
- They are aware and adhere to the AUP.
- They report any suspected misuse or problem to the people identified within this policy.
- All digital communications with students / pupils / parents / carers need to be carried out through a school medium and are of a professional nature.
- E-safety issues are embedded in all aspects of the curriculum and other activities when appropriate, if a form tutor they should deliver e-safety material when issued with it and ensure their knowledge is maintained for this interaction.
- Enforces any acceptable use policies with students and ensures that students are aware of acceptable e-safety standards.
- Within the relevant curriculum areas, they ensure that students have a good understanding of research skills and the need to avoid plagiarism.
- 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, for example supervised use in common rooms.
- Devices may not be used around the Academies including in corridors, in the yard, classrooms, etc and must be:
  - Confiscated from lower school students if seen in any of these areas, taken with the name of the child to Student Reception
  - Requested to be put away by sixth formers (at Southmoor)
- In lessons where internet use is pre-planned, pupils are guided as to what sites are appropriate for their use and if content that is not appropriate is found staff should:
  - Request students leave that particular website
  - Inform the technician (by email) of the user name of the student, the time they used the internet and a description of what was inappropriate about the site for investigation.

Students:

- Are responsible for using the Trust's digital technology systems in accordance with the Acceptable Use Policy.

- Need to understand the importance of reporting abuse, misuse or inappropriate materials to members of staff within school time and to know what to do outside of school time.
- 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.
- Should understand the importance of adopting good e-safety practice when using digital technologies outside of school and realise that the Trust's E-Safety Policy covers their actions outside of school, if related to their membership of the school.

Parents / Carers:

Parents / Carers are crucial to ensuring that children use the internet/mobile devices responsibly. The Trust will take every opportunity to help parents understand these issues through appropriate medium e.g. Headteacher's Blog. Parents and carers will be encouraged to support the Trust in promoting good e-safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events and agreements within the home school agreement
- access to relevant sections of the school website for further information about e-safety
- their children's personal devices in the school / academy

Policy Statements

Education – Students

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. This will ensure that when students are using ICT within and outside of school they do so responsibly and they are able to deal with any e-safety situations resiliently.

E-safety should be a focus in all areas of the curriculum when appropriate and staff should reinforce e-safety messages across the curriculum. The e-safety curriculum should be broad, relevant and provide opportunities for informed discussions:

- A planned e-safety curriculum should be provided as part of Computing, Personal Development and other lessons where appropriate (e.g. Drama).
- Key e-safety messages should be reinforced as part of a planned programme of assemblies.
- Students should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.
- Students should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet when appropriate.
- Students should be helped to understand the need for the Acceptable Use Policy and should be 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 / pupils should be monitored and any concerns addressed as detailed above.
- 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 (eg racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (or other

relevant designated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

Education & Training – Staff

It is essential that all staff receive regular independent e-safety training and internal training in order to understand their responsibilities, as outlined in this policy.

- Training should be pre-planned within the formal programme of staff training.
- All new staff should receive safeguarding training when starting employment with the Trust where e-safety best practice should be discussed.
- Designated persons should share relevant updates (e.g. KCSIE) at relevant times of the year.
- This E-Safety policy and its updates will be shared with staff for their discernment.
- The Designated Persons will provide advice / guidance / training to individuals as required and if requested.

Education & Training – Board of Trustees / Academy Council (Local Governors)

Trustees / Governors should take part in e-safety training where appropriate, this may fall in line with safeguarding training.

- Attendance at training provided if available by a relevant organisation.
- Participation in school training when appropriate.

Technical – infrastructure / equipment, filtering and monitoring

The Trust will be responsible for ensuring that the school infrastructure, network and devices are as safe and secure as is reasonably possible and as previously outlined. The technician must ensure that procedures approved within this policy are implemented.

- Trust technical systems will be managed in ways that ensure that the Trust meets recommended technical requirements.
- There will be reviews, tests and audits of the safety and security of Trust technical systems.
- Servers, wireless systems and cabling must be securely located and physical access restricted such as through locked doors, CCTV systems where appropriate.
- All users will have clearly defined access rights to school technical systems, network areas/resources and devices, these access rights are hierarchical by nature.
- All users will be provided with a username and secure password by the network technician 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 periodically.
- The administrator passwords for the Trust ICT system, used by the network technician, must also be available to the Headteacher and other nominated senior leaders, but, should be kept in a secure place (e.g. central safe).
- The network technician is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations.
- Internet access is filtered for all users. Illegal content (including child sexual abuse images) is filtered, appropriate content lists are regularly updated.
- The Trust has provided differentiated user-level filtering as appropriate.
- Trust technical staff monitor and the activity of users on the school technical systems when appropriate and users are made aware of this in the Acceptable Use Policy.
- Appropriate security measures are in place to protect ICT infrastructure from accidental or malicious attempts which might threaten the security of the Trust systems and data.

- An agreed policy is in place for the provision of temporary access of "guests" (eg trainee teachers, supply teachers, visitors) onto the Trust systems.
- An agreed policy is in place regarding the extent of personal use that users (staff / students / pupils / community users) and their family members are allowed on Trust devices that may be used out of school.
    - Devices if provided are predominately to be used for work purposes.
    - Members of staff may wish to use devices within their home as they would use personal devices for any work related and professionally acceptable recreational activities. - The above applies to sixth form students who are issued with tablets.
- Removable media (eg CDs/DVDs) but not memory sticks can be used by users on Trust devices. Sensitive data cannot be sent over the internet or taken off the Trust site unless safely encrypted or otherwise secured.

Bring Your Own Device (BYOD)

BYOD, or bring your own device, refers to the Trust E-safety policy that determines when and how employees, contractors and other authorised end users can use their own laptops, smartphones, and other personal devices on the Trust BYOD network to access corporate data and perform their job duties and to assist in education.

The contents of Trust systems and Trust data remain Trust property. This covers all materials, data, communications, and information, including but not limited to, Trust e-mail (both outgoing and incoming). Social media postings and activities, created on, transmitted to, received, or printed from, or stored or recorded on a device during the course of your work for the Trust or on its behalf is the property of the Trust, regardless of who owns the device.

The Trust reserves the right to refuse access to particular personally owned devices or software where it considers that there is a security risk to its systems and infrastructure. While the IT department will always endeavor to assist colleagues wherever possible, the Trust cannot take responsibility for supporting non-Trust managed devices.

User Responsibilities:

- All individuals who make use of BYOD must take responsibility for their own device and how they use it.
- They must: Familiarise themselves with their device and its security features so that they can ensure the safety of Trust information (as well as their own information).
- Invoke the relevant security features for the device.
- Maintain the device themselves ensuring it is regularly patched and upgraded using updates provided by vendors. Ensure that the device is not used for any purpose that would be at odds with the Trust IT regulations of use especially when it is on site or connected to the Trust network.

All users of BYOD must take all reasonable steps to:

- Prevent theft and loss of data.
- Keep information confidential where appropriate.
- Maintain the integrity of data and information, and take responsibility for any software they download onto their device.
- Ensure that software on personally owned devices is appropriately licenced.
- Encrypt documents or devices, as necessary.
- Not hold any information that is sensitive, personal, confidential, or of commercial value on personally owned devices. Instead, they should use their device to make use of the facilities provided to access to information securely over the internet.
- Be aware of any Data Protection issues and ensure personal data is handled appropriately.
- Report any security breach immediately.

- Ensure that no Trust information is left on any personal device indefinitely and make sure data is removed before a device is disposed of, sold, or transferred to a third party.
- Not keep any information longer than is necessary.

The Trust will not routinely monitor personal devices. However, it does reserve the right to prevent access to a particular device from either the wired or wireless networks or both.

Student use:
No student from lower school is permitted to use the BYOD Wi-Fi in any circumstances.
Sixth form students are permitted to use the BYOD Wi-Fi but must adhere to the guidance stated in this e-safety policy.

Use of digital and video images

Digital imaging allows staff, students and the Trust community to see the great work completed at our academies. In order to ensure that digital images use within the Trust environment are done so with care, the following principles must be adhered to:

- Students should be educated about the risks associated to using digital images including the distribution of images and publishing of personal images on social media, this should include referring to sexting and sending of inappropriate/nude/naked images.
- The Information Commissioner's Office states that parents and carers can take videos and digital images of their children at school events for their own personal use (as such use is not covered by the Data Protection Act). The Trust requests that 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. The Trust may prohibit this option at events and make available to parents / carers images / videos taken by the academy in which case, parents/carers will be requested not to take footage.
- Staff are allowed to take digital / video images to support educational aims. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes.
- 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 Trust into disrepute.
- Students must not take, use, share, publish or distribute images of others without their permission.
- Photographs published on the website, Headteacher's Blog or elsewhere, that include students, will be selected carefully and will comply with good practice guidance on the use of such images.
- Written permission from parents or carers is obtained by the home school agreement, the school will assume that parents and carers consent to images been taken in the case where the home school agreement has not been returned within a timely period

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 Trust 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 and lawfully processed.
- We work within the constraints of the Data Protection Act.
- Data subjects have rights of access and there are clear procedures for this to be obtained and there is a freedom of information statement.
- There are clear and understood routines for the deletion and disposal of data.
- Information and data risk incidents need to be logged and managed by the network technician.
- There are clear Data Protection clauses in all contracts where personal data may be passed to third parties.
- All policies relating to cloud storage and data protection adhere to the above and the technician has overall responsibility for ensuring the security of cloud storage.

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.
- Staff should back up their work regularly and technicians should perform central back-ups.
- 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.

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

- the data must be encrypted and password protected.
- the device must be password protected and the password should be regularly changed.
- the device must offer approved virus and malware checking software.
- the data must be securely deleted from the device, in line with school policy on data protection.
- portable devices should be stored appropriately.

Communications and acceptable use

Aspire North East Multi Academy Trust makes full use of ever developing commination technologies and appreciates that these technologies can enhance learning. The following table shows how the Trust currently considers the benefit of using these technologies for education outweighs their risks / disadvantages:

Communication Technologies	Staff			Students			
	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission
Mobile phones may be brought to school	x				x		
Use of mobile phones in lessons		x	x				x
Use of mobile phones in social time	x						x
Taking photos on mobile phones / cameras						x	
Use of other mobile devices eg tablets, gaming devices	x						x
Use of personal email addresses in school, or on school network		x				x	
Use of school email for personal emails		x		x			
Use of messaging apps		x		x			
Use of social media			x	x			
Use of blogs			x	x			

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

- The official Trust email service may be regarded as safe and secure and is monitored. Users should be aware that email communications may be monitored.
- Users must immediately report, to the lead technician and senior leaders 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 must be professional in tone and content. Staff should avoid email communication with parents where possible choosing to telephone parents.
- Group email addresses may be set up for information that is to be shared with whole classes, especially post-16 classes.
- 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 websites of the academies within the Trust and only official email addresses should be used to identify members of staff.

Social Media - Protecting Professional Identity

The teaching standards document identifies in Part 2 professional standards, these must be adhered to by staff when using social media.

Our duty of care is to provide a safe learning and working environment for pupils and staff. Vicarious liability demonstrates that our Trust 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 Trust liable to the injured party. Reasonable steps to prevent predictable harm must be in place and the school expects staff to avoid posting such material in accordance to the staff code of conduct.

The Trust provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the Trust 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
- Access to third party support where the case is deemed too complex for the school to deal with (ie legal services, police)

Trust staff should ensure that:

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

Unsuitable / inappropriate activities - acceptable use

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 Trust equipment or systems. The Trust policy restricts usage as follows:

User Actions

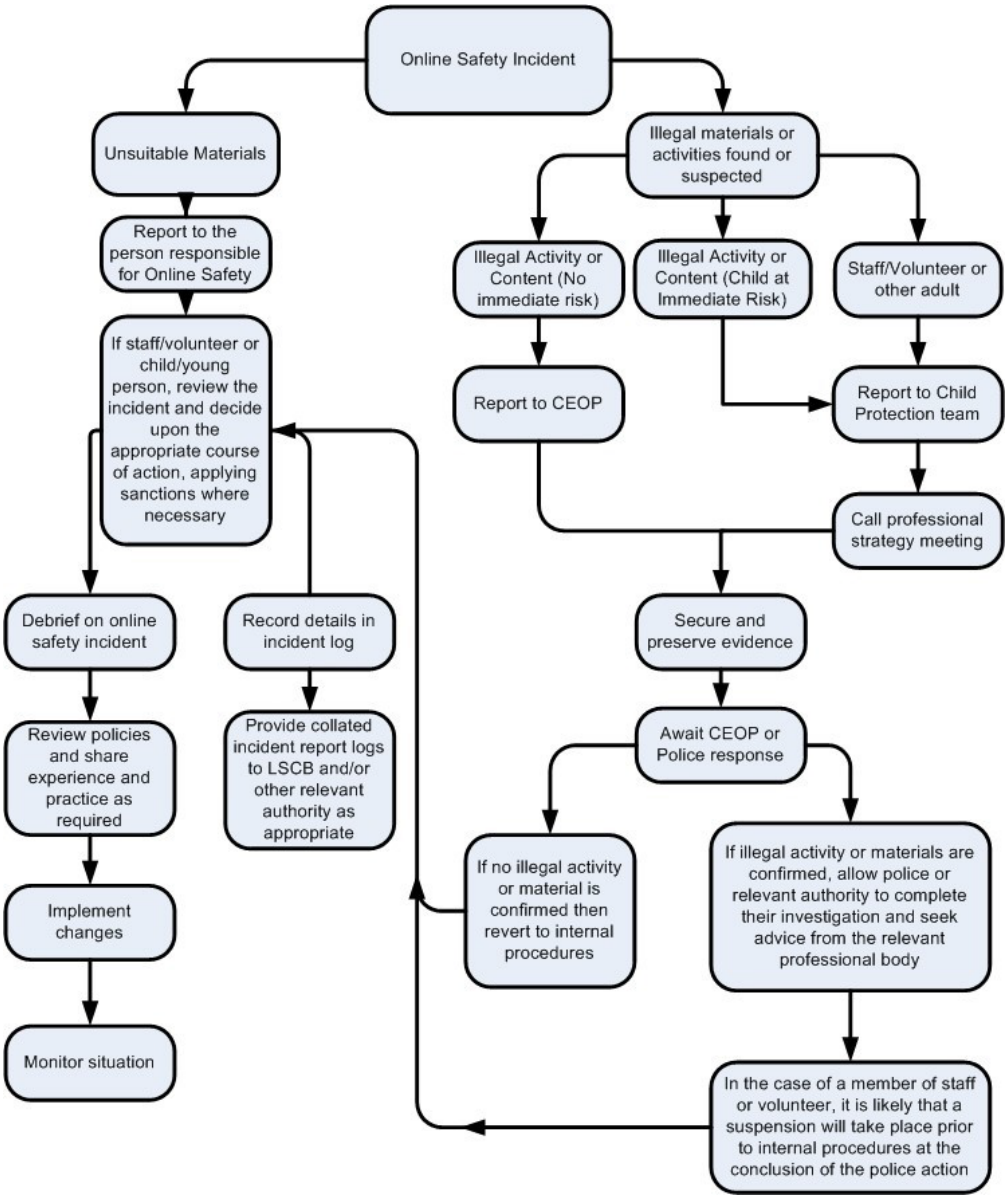
		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	Child sexual abuse 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	X
	Threatening behaviour, including promotion of physical violence or mental harm				X	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	X
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)					X	X
Creating or propagating computer viruses or other harmful files					X	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

Aspire North East Multi Academy Trust will use the following guidance in order to manage incidents that involve the use of online services. This will ensure a consistent approach to handling such incidents.

Illegal Incidents

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



Other Incidents

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

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

- Have more than one senior member of staff involved in the investigation 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).
- Once this has been completed and fully investigated a judgement as to whether this concern has substance or not must be made. If it does, then appropriate action will be required and could include the following:
    - Internal response or discipline procedures in accordance to staff conduct
    - Police involvement and/or action
- If content being reviewed includes images of child abuse, 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 a consistent trail of evidence trail for the Trust and possibly the police and demonstrate that visits to these sites were carried out for child protection purposes.

Trust / Academy Actions & Sanctions

It is more likely that the Trust 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 an appropriate manner, and that members of the Trust 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:

Students / Pupils Actions / Sanctions

Incidents:	Refer to Head of Department / Year Leader	Refer to Headteacher	Refer to Police	Refer to technical support staff for action re filtering / security etc	Inform parents / carers	Removal of network / internet access rig hts	Warning	Further sanction eg detention / exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).	X	X	X	X	X	X	X	X
Unauthorised use of non-educational sites during lessons	X							X
Unauthorised use of mobile phone / digital camera / other mobile device	X							X
Unauthorised use of social media / messaging apps / personal email	X							X
Unauthorised downloading or uploading of files	X							X
Allowing others to access school / academy network by sharing username and passwords	X	X		X	X			X
Attempting to access or accessing the academy network, using another student's / pupil's account	X				X			X
Attempting to access or accessing the academy network, using the account of a member of staff	X	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
Continued infringements of the above, following previous warnings or sanctions		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		X	X
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act	X	X	X	X	X	X	X	X

Staff Actions / Sanctions

Incidents:	Refer to line managerr	Refer to Headteacher	Refer 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		X	X	X	x	x		x
Inappropriate personal use of the internet / social media / personal email	x							
Unauthorised downloading or uploading of files	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	x	x		x
Careless use of personal data eg holding or transferring data in an insecure manner	x				x			
Deliberate actions to breach data protection or network security rules		x	x	x	x			x
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		x	x	x	x			x
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	x							
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils		x	x			x		x
Actions which could compromise the staff member's professional standing	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
Using proxy sites or other means to subvert the school's / academy's filtering system	x	x	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	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

Acknowledgements: Aspire North East Multi Academy Trust would like to acknowledge the use of SWGfL E-Safety Self Review Tool

Disclaimer: The content of this policy is accurate as of the date of publication.