Midsomer Norton Schools Partnership

Issued:	September 2024
Review:	Term 1 annually
LST:	MLY

ONLINE SAFETY POLICY

1 Scope of the Policy

This policy applies to all members of the Midsomer Norton Schools' Partnership Trust (known from now on as the 'Trust') community (including staff, students / pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of any MAT digital technology systems, both in and out of any school within the Trust.

Whilst the internet and associated technologies are an excellent tool and resource to enrich learning there are still dangers related to their use, especially in relation to young students. Some examples of this are:

- Bullying via chat or email
- Obsessive internet use
- Exposure to inappropriate materials
- Inappropriate or illegal behaviour
- Physical danger of sexual abuse

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

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

It is our duty of care alongside that of parents and other members of the community, to protect our students from the dangers they become exposed to while using online resources, and this can be achieved by many different mechanisms working together. The purpose of this e-safety policy is to outline what measures the Trust takes to ensure that students can work in an e-safe environment and that any e-safety issue is detected and dealt with in a timely and appropriate fashion.

This E-Safety policy encompasses any electronic device that is capable of recording, storing, transferring or publishing any digital media. It includes, but is not limited to, mobile phones, laptop computers, desktop computers, tablet PC, media recorders (MP3 players) and game consoles as well as other collaboration tools and personal publishing tools. This policy highlights the need to educate students about the benefits and risks of using technology and provides safeguards and an awareness for users to enable them to control their online experience in a safe and meaningful way.

The Trust e-safety policy should be read in conjunction with other policies including, but not limited to, AUP for ICT, Mobile Phone Policy, Student Behaviour, Anti-Bullying, Curriculum, Child Protection, Safeguarding, Data

Protection and Security and the use of Children's Images. This policy supplements all current legislation applicable to schools including the PREVENT duty as outlined in the Counter-Terrorism and Security Act 2015.

2 Roles and Responsibilities

The following section outlines the online safety roles and responsibilities of individuals and groups within the Trust.

2.1 Trust Board

Trust Board members are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy.

2.2 Headteacher and Senior Leaders

- The Headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day to day responsibility for online safety may be delegated to another member of the SLT.
- The Headteacher and (at least) another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff. (see flow chart on dealing with online safety incidents "Responding to incidents of misuse" and relevant Trust disciplinary procedures).
- The Headteacher / Senior Leaders are responsible for ensuring that staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.
- The Trust Director of IT will ensure that there is a system in place to allow for monitoring online safety.
- The Headteacher and School Leaders should ensure that all pupils are taught about online safety as part of the planned curriculum at least annually.

2.3 Network Manager / Technical staff

The Network Technical Staff are responsible for ensuring:

- That the school's technical infrastructure is secure and is not open to misuse or malicious attack
- That the school meets required online safety technical requirements
- That users may only access the networks and devices through a properly enforced password protection policy, (See Trust Password Policy)
- The filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person
- That they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform, share and update others as relevant
- That the use of the network / internet / remote access / email is regularly monitored in order that any misuse/attempted misuse can be reported to the Headteacher for investigation / action / sanction
- That monitoring software / systems are implemented and updated as agreed in school / academy policies

2.4 All staff (Teaching and non-teaching)

Are responsible for ensuring that:

- They have an up to date awareness of online safety matters and of the current MAT Online Safety Policy and practices
- They have read, understood and signed the Staff Acceptable Use Policy (AUP)
- They report any suspected misuse or problem to the Headteacher or Senior Member of Staff for investigation / action / sanction
- All digital communications with students / pupils / parents / carers should be on a professional level and only carried out using official school systems
- Ensure that online safety issues are embedded in all aspects of the curriculum and other activities, and to remind students at every possible opportunity when their work involves the use of ICT
- Students / pupils understand and follow the Online Safety Policy and acceptable use policies
- Students / pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations

- They monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities (where allowed) and implement current policies with regard to these devices. Where available, staff MUST use monitoring software when in IT rooms to ensure students are on task and not at risk.
- In lessons where internet use is pre-planned pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Ensuring that where sound and video media that is based on streaming services, its use is pre-planned and that the whole material has been checked as being suitable for the age of the students that are accessing the material.

2.5 Designated Safeguarding Lead or Designated Persons

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

- Sharing of personal data
- Access to illegal / inappropriate materials
- Inappropriate on-line contact with adults / strangers
- Potential or actual incidents of grooming
- Online-bullying

2.6 Students / Pupils:

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

2.7 Parents/Carers

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet and mobile devices in an appropriate way. Schools will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, and information about national or local online safety campaigns. Parents and carers will be encouraged to support the school in promoting good online safety practice and to follow guidelines on the appropriate use of:

- Digital and video images taken at school events
- Access to parents' sections of the website and on-line pupil records
- Their children's personal devices in the school

2.8 Community Users

Community Users who access school systems as part of the wider school provision will be expected to sign an Acceptable User Policy. Community users could include volunteer persons coming to run clubs for students within the school.

Community users will accept that no alteration can be made to existing systems that would potentially reduce the effectiveness of security systems in place in the school or that may introduce vulnerabilities that could be exploited.

External agencies or support who use the system to deliver extra curricular activities must accept that no alteration can be made to existing systems that would potentially reduce the effectiveness of security systems in place in the school or that may introduce vulnerabilities that could be exploited.

3 Education

3.1 Why Internet use is important

The Internet is an essential element in 21st century life for education, business and social interaction. Each school has a duty to provide students with quality Internet access as part of their learning experience.

Internet use is a part of the curriculum and a necessary tool for staff and pupils. Students use the Internet widely outside school on a range of devices and it is important that they learn how to evaluate Internet sources, identify potentially harmful situations and to take care of their own safety and security.

3.2 Internet use will enhance learning

The Internet access provided by the Trust has been tailored expressly for pupil and staff use and will include appropriate filtering. It is important to bear in mind that with the ever changing nature of the Internet the filtering provided by the Trust cannot be guaranteed to be 100% effective and all adults should be continually aware of the need to be vigilant when students are using technologies to access on-line materials.

Students should be taught what Internet use is acceptable and what is not and given clear objectives for Internet use when it is being used in lessons. To this end all Internet access will be planned to enrich and extend learning activities. Trust Staff should guide pupils in on-line activities that will support the learning outcomes planned for the Students' age and maturity.

Students will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation, and staff will make use of any technologies in place to monitor and restrict access to Internet resources so that its use is focused and controlled.

3.3 Pupils will be taught how to evaluate Internet content

The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law. Students should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy. Students should be taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work, regardless of their age.

3.4 How will pupils learn to use ICT appropriately?

If students are to be as safe at home as they are at school, they need to recognise the risks for themselves. Each school will have a programme of teaching appropriate skills in the early years which will reinforce the safe and appropriate use of the Internet. These skills will be revisited by staff when they use ICT to support the teaching and learning. It is the responsibility of ALL staff to ensure that any use of ICT by students is appropriate.
The understanding of appropriateness will be further developed through the PSHE/learning for life curriculum and assemblies which should further develop the students understanding of the risks and opportunities of using the Internet, and social networking sites.

3.5 Pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in online safety and digital literacy is therefore an essential part of the school's online safety provision. All schools will have a program of study embedded into their curriculum that will allow all pupils to understand the dangers and opportunities of online usage. Children and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience.

Online safety should be a focus in all areas of the curriculum (and not the sole responsibility of those teaching IT) and staff should reinforce online safety messages across the curriculum. The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned online safety curriculum should be provided as part of Computing/PHSE/other lessons and should be regularly revisited

- Key online safety messages should be reinforced as part of a planned programme of assemblies and tutorial and pastoral activities
- Pupils should be taught in all lessons to be critically aware of the materials and content they access on-line and be guided to validate the accuracy of information.
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Pupils should be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making.
- Pupils should be helped to understand the need for the Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school.
- Staff should act as good role models in their use of digital technologies, the internet and mobile devices
- In lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites that have been checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches. Below Key Stage 4, it is not good practice to simply allow students to "search the Internet" for resources. By the time pupils have reached Key Stage 4, they should be competent to undertake research that is safe. Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.
- It is accepted that from time to time, for good educational reasons, pupils may need to research topics (eg racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

3.6 Parents / Carers

Many parents and carers have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring and regulation of the children's online behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The school will therefore seek to provide information and awareness to parents and carers through a range of activities, including but not limited to:

- Curriculum activities
- Letters, newsletters, web site, Learning Platform
- Parents / Carers evenings / sessions
- High profile events / campaigns e.g. Safer Internet Day
- Reference to the relevant web sites and publications
- Sharing material that has been distributed via the Trust that has been designated as needing to be shared with parents and carers.

3.7 Education & Training – Staff / Volunteers

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

- A planned programme of formal online safety training will be made available to staff. This should be regularly updated and reinforced. An audit of the online safety training needs of all staff will be held on the Single Central Record.
- All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the school Online Safety Policy and Acceptable Use Agreements.
- It is expected that some staff will identify online safety as a training need within the performance management process.

3.8 Training – Governors / Directors

Governors and Board members should take part in online safety training and awareness sessions, with particular importance for those who are members of any subcommittee or group involved in technology and online safety, health and safety or safeguarding.

4 Managing Internet Access

4.1 Information system security

- The capacity and security of the ICT systems provided by the Trust will be reviewed regularly;
- Virus protection will be automatically updated regularly;
- Where computers have access to sensitive financial data over the Internet, additional security software will be installed to protect the finances of the Trust.

4.2 E-mail

- All emails sent from the ICT systems within the Trust to external bodies will encompass a standard footer statement
- Students may only use approved e-mail accounts on the school system.
- Students must immediately tell a teacher if they receive an offensive e-mail.
- Students must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- E-mail sent to an external organisation by pupils should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.
- The forwarding of chain letters is not permitted.
- Where necessary a Whole-class or group e-mail addresses should be used at Key Stage 2 and below;
- Access in school to external personal e-mail accounts may be blocked. This is because it will not be secure and conform to the relevant legislation governing security of data.
- Emails are scanned and some emails may be quarantined as the software may suspect the content or the attachment. The IT teams can release these emails BUT only after action has been taken to prove the identity of the sender. This is best achieved by contacting the sender, explaining the email has been trapped, and asking for it to be sent again. This will prove that the email is not a spoofed email. If it is trapped again IT will know it is legitimate and release it.
- No one should open any attachment or follow any link within an email if they do not recognise the sender. The best advice is if the user is unsure, delete the email.

4.3 Published content and the school Website

- The contact details on the individual school Websites will be the school address, e-mail and telephone number.
- Staff or students' personal information will not be published.
- Each school should designate a person with overall editorial responsibility and ensure that content on the school's website is accurate and appropriate.

4.4 Publishing pupil's images and work

- Photographs that include students will be selected carefully and will not enable individual students to be identified by name. These will be vetted by a member of the leadership team;
- Student's full names will not be used anywhere on any Website or Blog, particularly in association with photographs;
- Each school will record on the MIS system all parents who object to their children's pictures being used in publicity;
- Written permission from parents or carers will be obtained before photographs of students are published on any website;
- Student work can only be published with the permission of the student.

Staff should refer to the Trust Data Protection Policy before using any pupil images internally or externally.

4.5 Managing filtering

- Smoothwall, RM Safety Net, Netsweeper or Lightspeed provide real time filtering using Dynamic Content Analysis. All pages are content filtered using the Dynamic Content Analysis Engine, which analyses all page contents in real time and as it does this, it builds up content categorisation. The system scans the content, context and construction of web pages in detail. This means that sites not previously visited or seen by the filtering system can be categorised in real time.
- The recommendation is that filtering should not be an in-house solution. Where new schools joint the MAT, they are given period of grace until their existing support contracts expire, and the expectation is

that they then move to the current Cloud based supported MAT solution, usually a managed service provided by a 3rd party. Having an externally provided solution will allow for continuity of service in the event of technicians moving on from their current role.

- The MAT solution should allow for the ability to filter by user, user type, group and device used.
- Where the Trust oversees the filtering, it will ensure that the systems in place to protect pupils are reviewed and improved on an annual basis as necessary;
- The Trust will proactively add inappropriate websites to the filter lists as appropriate. Unblocking may only be permitted once the site has been discussed with a senior member of staff and this authorisation then communicated in writing to the technical team. Users need to be aware that this process is not immediate and it is recommended that at least 2 days notice is given of any change request to be processed.
- If staff or students discover an unsuitable site, it must be reported to a member of the ICT support teams who will then take the appropriate action. In certain circumstances they may filter the site immediately until a review of the site can be undertaken;
- ICT Support staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable;
- Any material that the school believes is illegal will be reported to the Headteacher in the first instance. Should it be necessary, this will then be passed to the relevant authorities.

4.6 Managing Firewalls

- Due to the significant potential risks involved with running networks, all firewalls will be part of a managed service where the service provider will undertake the management and risk of managing the firewall. Schools should not have their own hardware based firewall in school.
- Schools that are new to the MAT will be given a grace period until their existing support contract has expired.

4.7 Managing emerging technologies

- Technologies are continually changing and emerging. Whilst it is not possible to cover all such devices, it is intended that the policies of the Trust have been written in such a way that they cover newest technologies;
- There is a separate Mobile Devices Policy which addresses their use within the school environment. This policy also covers the use of mobile devices whilst on any trip organised by the school;
- Students need to be aware that the sending of abusive or inappropriate text messages is forbidden and will be dealt with under the guidance of the individual schools Behaviour Policy;
- Staff will be issued with a school mobile phone where contact with pupils is required for example on foreign trips or outward bound activities. Staff should not issue their personal phone numbers to students;
- The use of portable media devices including for example the iTouch is acceptable so long as use is appropriate. Wireless access points have been provided by the Trust in each school to encourage the students to use them to support their studies. The Internet access afforded through these devices is via the normal filtered Internet Access.

4.8 Protecting personal data

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018. Any misuse of data must be reported to the safety coordinator immediately;
- Staff will ensure that they lock the terminal should they need to be away from their desk to prevent unauthorised access to student data;
- Student data can only be uploaded to recognised safe and secure cloud storage as defined by Her Majesty's Government. Currently the only two ratified safe and secure cloud storage are: Microsoft One Drive and Google Education accounts. Personal Google accounts are NOT secure under the terms of the Data Protection Act 1998.
- Student data taken home must be protected by suitable means;
- Some schools in the Trust will be able to share student data via the Web. Where this is the case it will only be shared with parents/guardians with a priority setting of 1 or 2. All accounts will be secured by username and password;
- The school will undertake appropriate backups to protect the personal data on the computer network.

- Where schools are required to transfer data to other organisations, eg exam boards, local authority, this MUST be done using the provided secure data transfer mechanisms. In lots of cases, Globalscape is used. Data MUST not be transferred openly in emails or as unencrypted attachments.

4.9 Cloud Storage

Employees of the Trust must note that:

- Not all cloud based storage technologies are safe and secure. The Trust follows the guidance provided by the DFES and at the time of review, the only recognised cloud storage permissible by the staff in the Trust are Google Drive and Microsoft One drive. The MAT default preferred storage is Google Drive.
- Staff should not store any other data related to their day-to-day work in any other cloud based systems without first discussing this with the Director of ICT.

5 Social Media - Protecting Professional Identity

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

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

- Ensuring that personal information is not published
- Training is provided including: 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
- Communications with pupils and parents to advise them that the use of social network spaces outside school can be dangerous
- A program of education that reinforces to students that they must never give out personal details online.

School staff should ensure that:

- No reference should be made in social media to pupils, parents or carers or school staff
- They do not engage in online discussion on personal matters relating to members of the school community
- Staff must not under any circumstances communicate with any student through social networking sites
- Staff will be advised not to have social network sites, but where they do they must be secure, and must not have any ‘friend’ that is a current of ex-student.
- Personal opinions should not be attributed to the school or the Trust.
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information

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

- A process for approval by senior leaders
- Clear processes for the administration and monitoring of these accounts – involving at least two members of staff
- A code of behaviour for users of the accounts, including:
    - Systems for reporting and dealing with abuse and misuse
    - Understanding of how incidents may be dealt with under school disciplinary procedures

6 Policy Decisions

6.1 Authorising Internet and email access

- All users of the system must read and sign the ‘Acceptable Use Policy’ before using any ICT resource. Parents will be asked to counter sign and return the student AUP form. (Some schools may have the form in the front of the student planner. It is suggested that a paper copy is also kept on the student’s record in the pastoral office).

- Upon leaving the school the accounts for both Staff and students will be disabled for a period before being deleted.

6.2 Assessing risks

- Where the Trust manages the internet and filtering provision, it will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a computer within the Trust.
- The Trust will audit ICT provision to establish if the e-safety policy is adequate and that its implementation is effective.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.

6.3 Community use of the Internet

- The Trust will liaise with local organisations to establish a common approach to e-safety. Special accounts may be set up specifically for community use;
- The Trust may not afford access to the Internet by any external contractors for any reason as it breaches security and firewall procedures.

7 e-Safety Violations

7.1 Handling e-safety complaints

- Complaints of Internet or email misuse by students will be investigated and supervised by a member of the Pastoral care team or Headteacher, who may implement any relevant punishment, which could include bans for either Internet or email or both. Letters will be sent to parent and carers outlining the offence and the sanctions imposed. A record of this misuse will be logged on the School's MIS system;
- Complaints of Internet or email misuse by staff will be referred to the head teacher;
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.

7.2 Abuse of mobile devices and media within school

- The schools within the Trust will take a serious and robust approach to any misuse of technology which occurs on any site. If the abuse is via a mobile phone, the phone will immediately be confiscated and an investigation undertaken by a member of the pastoral care team or Headteacher. If the issue relates to inappropriate images, then the Safeguarding Lead must be immediately informed. In these circumstances staff must not under any circumstances view the images or forward them onto another person as this is an offence in its own right.
- Parents/guardians will be informed about the incident and any resulting actions taken as punishment;
- Where necessary, external agencies will be informed including the Police;
- All such incidents will be logged on the individual school's MIS system.

7.3 Abuse of mobile devices and media outside of school

- Although rare, it is an increasing occurrence where modern technology is used to cause offence and hurt outside of the school. Where the school becomes aware of the issue they will take a serious and robust approach to the misuse;
- Parents and carers will be informed about the incident and any resulting actions taken as punishment;
- Where necessary, external agencies will be informed including the Police;
- All such incidents will be logged on the individual school's MIS system.

8 Bring Your Own Device (BYOD):

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. This has led to the Trust encouraging students to bring their own technologies into the school environment, especially at Post 16, in order to provide a greater freedom of choice and usability. There are, however, a number of e-safety considerations for BYOD. The Trust is clear that the use of BYOD should not introduce vulnerabilities into

existing secure environments. For this reason, the Trust will extend any policy relating to the use of technologies to any device that is provided by the Trust or that is classed as a BYOD.

The Trust has a set of clear expectations and responsibilities for all users:

- All users adhere to the Data Protection Act principles.
- 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 ’s normal filtering systems, while being used on the premises.
- All users will use their username and password to access the ICT systems and Internet via a BYOD;
- Students are reminded that misuse of their own equipment is covered by the ’s policy as if it were a misuse of the ’s equipment.

9 Dealing with unsuitable / inappropriate activities

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

The Trust 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 or outside the 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	X
	Promotion of any kind of discrimination						X
	threatening behaviour, including promotion of physical violence or mental harm						X
	Promotion of extremism or terrorism						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	
User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal	

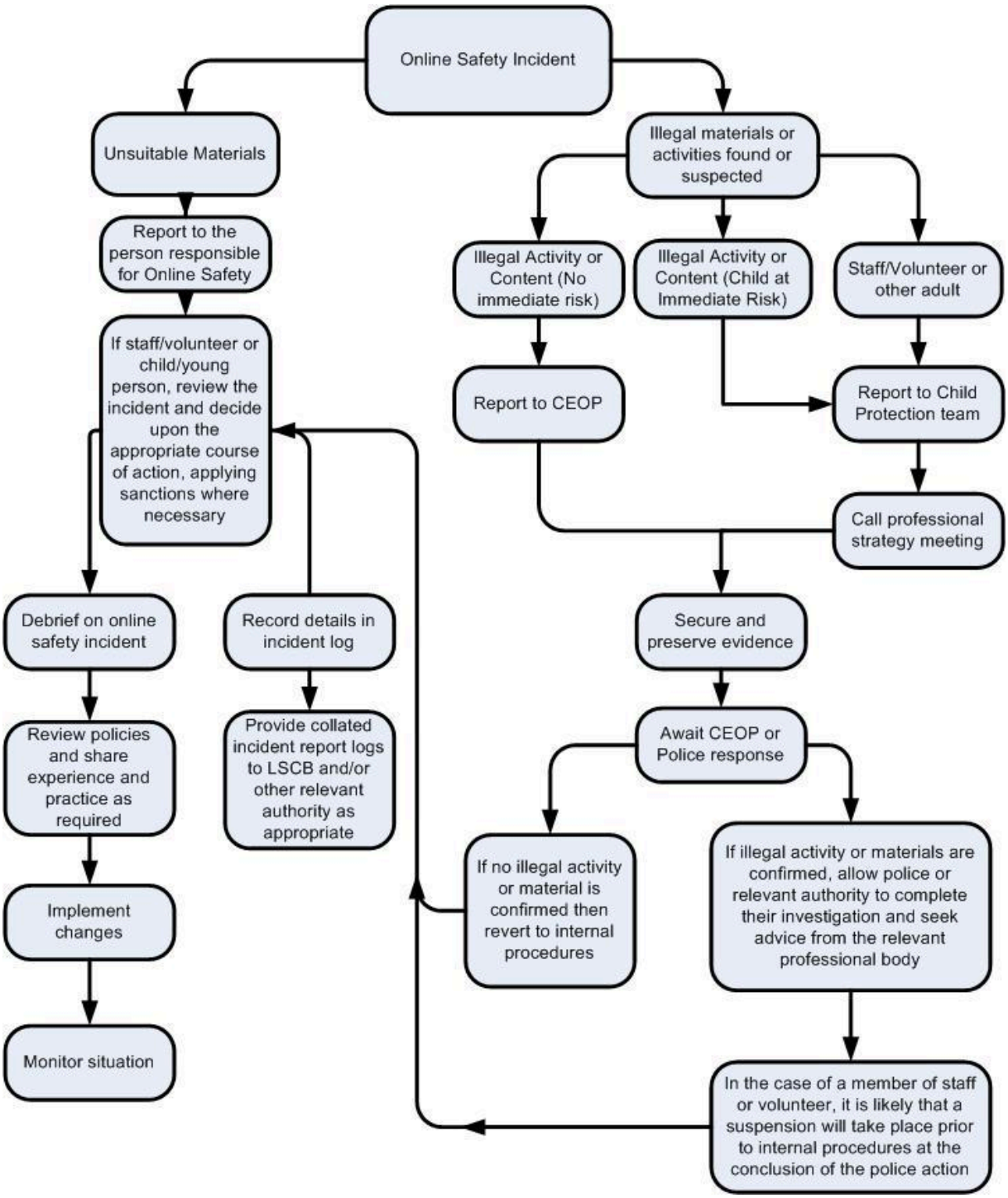
Creating or propagating computer viruses or other harmful files						X
Unfair usage (downloading / uploading large files that hinders others in their use of the internet, including streaming radio stations for personal use.)					X	
On-line gaming (educational)			X			
On-line gaming (non-educational)					X	
On-line gambling					X	
On-line shopping / commerce				X		
File sharing					X	
Use of social media				X		
Use of messaging apps				X		

10 Responding to incidents of misuse

This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities. Online Safety BOOST includes a comprehensive and interactive 'Incident Management Tool' that steps staff through how to respond, forms to complete and action to take when managing reported incidents (https://boost.swgfl.org.uk/)

10.1 Illegal Incidents

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



10.2 Other Incidents

It is hoped that all members of the school 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 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 / Academy Group or national / local organisation (as relevant).
    - Police involvement and/or action
- If content being reviewed includes images of child abuse, then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:
    - incidents of 'grooming' behaviour
    - the sending of obscene materials to a child
    - adult material which potentially breaches the Obscene Publications Act
    - criminally racist material
    - promotion of terrorism or extremism
    - 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 Trust and possibly the police and demonstrate that visits to these sites were carried out for safeguarding purposes. The completed form should be retained by the group for evidence and reference purposes.

11 Actions & Sanctions

It is more likely that the school 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.

12 Passwords

Passwords are an important aspect of computer security. They are the front line of protection for user accounts and the associated software used to manage the business of the Federation. This policy is kept simple so that the security of the system is maintained.

General Details – system access

- All system-level passwords (e.g., root, enable, NT admin, application administration accounts, etc.) must be changed on at least a bi-annual basis.

- Servers should have a local account enabled and have a different credential to a network admin user.
- All user-level passwords (e.g., email, desktop computer, etc.) must be changed at least every twelve months. This will be initiated automatically by the ICT support team.
- Users who have access to the financial data of the Trust will have a policy implemented which requires a password change on a more regular basis. (Auditor requirement)
- All cloud based accounts provided by the Trust (Google and Microsoft) will adhere to the complexities listed below
- Two factor authentication will be used on all admin accounts to cloud services.
- Passwords must not be inserted into email messages or other forms of electronic communication.
- All user accounts will have the ability to change passwords. The complexity and history is determined by the AD Policies. Currently:
    - Minimum of 10 characters
    - Minimum of 1 letter
    - Minimum of 1 number
    - Minimum of 1 capital letter
    - Cannot contain more than 2 consecutive letters of a username

<u>Password Protection Standards</u>

For other applications on the individual school networks the following should apply:

- Users should not use the same password for administrative applications (eg MIS system) and the main network system.
- Password MUST NOT be set to Password or combinations of it. Users are encouraged not to use the "Remember Password" feature of applications.
- Users are reminded not to write passwords down and store them anywhere in their office. Do not store passwords in a file on ANY computer system without encryption.
- Users must be aware of the following:
- Don't reveal a password over the phone to **ANYONE**
- Don't reveal a password in an email message
- Don't reveal a password to the boss
- Don't talk about a password in front of others
- Don't hint at the format of a password (e.g., "my family name")
- Don't reveal a password on questionnaires or security forms
- Don't share a password with family members
- Don't reveal a password to co-workers
- Staff **MUST NOT** under any circumstances allow a student to use any of their Logon credential to access any part to the Federation computer system.

<u>MIS Applications</u>

- The passwords to these systems should be different to those used to access the network, unless the system runs a ‘Single Sign-on’ facility.
- Password changes should be made whenever the main network passwords are changed, but remembering not to use the same password.
- Where a member of staff believes their password to be compromised it should be changed with immediate effect

<u>Student Passwords</u>

- The passwords for the students will conform to the network standard
- Their frequency of change is once per year
- If they forget their password it is reset for them, but they must change it upon logon.
- Staff have access to be able to change student passwords, they must tick the box to force the student to change their password upon new logon