Online Safety Policy
Myton School

Approved by:	Leadership Team	**Date:**	21 March 2023
Last reviewed on:	21 March 2023		
Next review due by:	21 March 2024		
Version	1		

Contents

Schedule for Monitoring / Review 2
Scope of the Policy 3
Roles and Responsibilities 3
Governors 3
Headteacher and Senior Leaders 3
Online Safety Officer 4
Network Manager 4
Teaching and Support Staff (Including Volunteers) 5
Designated Safeguarding Lead 6
Students: 6
Parents / Carers 7
Policy Statements 7
Education – Students 7
Education – Parents / Carers 8
Education & Training – Staff / Volunteers 8
Training – Governors 9
Technical – equipment, filtering and monitoring 9
Dealing with unsuitable / inappropriate activities 11
Responding to incidents of misuse 12
Illegal Incidents 12
Incidents requiring investigation 14

Schedule for Monitoring / Review

The implementation of this Online Safety policy will be monitored by the:	Online Safety Officer, Senior Leadership Team)
Current Online Safety Officer	Sean Johnson
Monitoring will take place at regular intervals:	Once a year
The Board Governors Body will receive a report on the implementation of the Online Safety Policy generated by the monitoring group (which will include anonymous details of online safety incidents) at regular intervals:	Once a year
The Online Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place. The next anticipated review date will be:	21 March 2024
Should serious online safety incidents take place, the following external persons / agencies should be informed:	LADO, MASH, PREVENT as appropriate. If in doubt, speak to safeguarding team

The school will monitor the impact of the policy using:

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

Scope of the Policy

This policy applies to all members of the Myton School (including staff, students, volunteers, parents and visitors) who have access to and are users of school digital technology systems, both in and out of Myton.

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of students when they are off the academy 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.

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

Roles and Responsibilities

The following section outlines the online safety roles and responsibilities of individuals and groups within Myton School:

Governors

Governors are responsible for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about online safety incidents and monitoring reports.

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 will be delegated to the Online Safety Officer.
- 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 – included in a later section – “Responding to incidents of misuse” and relevant Local Authority.

- The Headteacher is responsible for ensuring that the Online Safety Officer and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.
- The Headteacher will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- The Senior Leadership Team will receive regular monitoring reports from the Online Safety Officer once a term.

Online Safety Officer

- Takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies / documents
- Ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place
- Provides training and advice for staff
- Liaises with the Local Authority
- Liaises with school technical staff
- Receives reports of online safety incidents and either tracks these on CPOMS or, where the perpetrator/victim is unknown or the incident is cyberbullying/harassment of a teacher, creates a log of incidents to inform future online safety developments
- Meets regularly with governor with role Safeguarding Lead to discuss current issues, review incident logs and filtering / change control logs
- Attends relevant meetings of Governors
- Reports regularly to Senior Leadership Team
- Forwards any concerns from staff to the Safeguarding Team through CPOMS.

Network Manager

The Network Manager and the IT support team is 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 and any Local Authority Online Safety Policy or Guidance that may apply.

- That users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed.
- 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 and update others as relevant
- That the use of the network, remote access and email is regularly monitored in order that any misuse or attempted misuse can be reported to the Headteacher or Online Safety Officer for investigation.
- They have a copy of Social Media account details for the school that can be used to remove posts/videos if required.
- That monitoring software are implemented and updated as agreed in school policies.
- Receives and analyses daily reports of flagged internet usage and sends any concerns to safeguarding team through CPOMS.

Teaching and Support Staff (Including Volunteers)

Are responsible for ensuring that:

- They have an up to date awareness of online safety matters and of the current school Online Safety Policy and practices
- They have read, understood and signed the Staff Acceptable Use Policy (AUP)
- They report any suspected misuse or problem to the Online Safety Officer and, if the misuse or problem is a safeguarding issue, follow Myton's Child Protection and Safeguarding policy and inform the Safeguarding Team using CPOMS.
- If the victim and perpetrator are unknown, or the incident is cyberbullying/harassment of a member of staff with an unknown perpetrator, then they report the incident to the safeguarding team on the DLSafeguarding@myton.co.uk email address.
- All digital communications with students, parents and carers should be on a professional level and only carried out using official school systems and using software that requires a school login.

- Staff ensure that they logout or lock computers they are using that students could access, to ensure students don't access confidential information or misuse software.
- Online safety issues are embedded in all aspects of the curriculum and other activities.
- Students understand and follow the Online Safety Policy and acceptable use policies.
- They monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- In the case of recording a lesson for educational purposes, make students aware if a lesson is being recorded and, if these need to be uploaded online, upload them with a service that only allows members of Myton School to view it.

Designated Safeguarding Lead

Should be trained in Online Safety issues and be aware of the potential for serious 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

Students:

- Are responsible for using the school digital technology systems in accordance with the Student Acceptable Use Agreement
- 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 or using images and on online-bullying, as well as using streaming technology to link with classes.
- Will also be expected to practice good online etiquette while participating in online lessons and not put other students and staff in danger by, for example, taking screenshots of the lesson while a staff member or other student is on the screen, or inviting people to lessons.

- 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

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. Myton School will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website 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
- Their children's personal devices in the school (where this is allowed).

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 online safety and digital literacy is therefore an essential part of the school's online safety provision. Children and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience.

Online safety should be a focus in all areas of the curriculum and staff 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 and PHSE lessons in Key Stage 3 and in PSHE in Key Stage 4. These should be regularly revisited.
- Key online safety messages should be reinforced as part of a planned programme of assemblies and tutor activities.
- 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

- Students 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.
- Students should be helped to understand the need for the student Acceptable Use Policy 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.
- Where students are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit, if possible using the screen monitoring system (Currently Impero). If staff are not confident in using the system, extra training is provided.
- 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 can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

Education – Parents / Carers

Many parents and carers have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring 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.

Myton School will therefore seek to provide information and awareness to parents and carers through:

- Curriculum activities
- Letters, including the newsletter on the school website.
- Parents / Carers evenings
- High profile events / campaigns e.g. Safer Internet Day

Education & Training – Staff / Volunteers

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

- A planned programme of formal online safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out once a year.

- 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.
- Staff will be trained in how to use the school software to help them monitor student's activity while in lessons, i.e. Impero.
- It is expected that some staff will identify online safety as a training need within the performance management process.
- The Online Safety Officer will receive regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisations.
- This Online Safety Policy and its updates will be presented to staff in staff meetings / INSET days.
- The Online Safety Officer will provide advice and training to individuals or groups as required.

Training – Governors

The designated Governor in charge of Safeguarding should take part in online safety awareness sessions, which may be completed by the attendance at training provided by the Local Authority / MAT / National Governors Association / or other relevant organisation (e.g. SWGfL).

Technical – equipment, filtering and monitoring

The school will be responsible for ensuring that the 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 online safety responsibilities:

- School technical systems will be managed in ways that ensure that the school meets recommended technical requirements.
- There will be regular reviews and audits of the safety and security of school technical systems.
- Servers, wireless systems and cabling must be securely located and physical access restricted.
- All users will have clearly defined access rights to school technical systems and devices.
- All users will be provided with a username and secure password during their first fortnight at the school. Users are responsible for the security of their username and password.

- The “administrator” passwords for the school ICT systems, used by the Network Manager must also be available to the Headteacher or some other nominated senior leader and kept in a secure place.
- The Network Manager is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations.
- Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored. There is a clear process in place to deal with requests for filtering changes.
- Internet filtering / monitoring should ensure that children are safe from terrorist and extremist material when accessing the internet.
- The school provides differentiated user-level filtering for staff and students
- School technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement.
- An appropriate system is in place for users to report any actual technical incident / security breach to the relevant person.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software.
- An agreed policy is in place where special accounts exist for the provision of temporary access of “guests” (eg trainee teachers, supply teachers, visitors) onto the school systems.
- An agreed policy is in place regarding the use of removable media (eg memory sticks / CDs / DVDs) by users on school devices. Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.
- Recording online lessons is not an expectation from teachers and should only be used for educational purposes, not monitoring.

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.

Myton 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 or outside the school when using school equipment or systems. The school policy restricts usage as follows:

The following are unacceptable:

- Using school systems to run a private business
- Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school
- Infringing copyright
- Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)
- Creating or propagating computer viruses or other harmful files
- Visiting Internet sites, making, posting, downloading, uploading, data transferring, communicating or passing on material, remarks, proposals or comments that contain or relate to:
    - Pornography
    - Promotion of any kind of discrimination
    - threatening behaviour, including promotion of physical violence or mental harm
    - Promotion of extremism or terrorism
    - Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute

The following are unacceptable and illegal:

- Visiting Internet sites, making, posting, downloading, uploading, data transferring, communicating or passing 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
    - Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.

- Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008
- Criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986

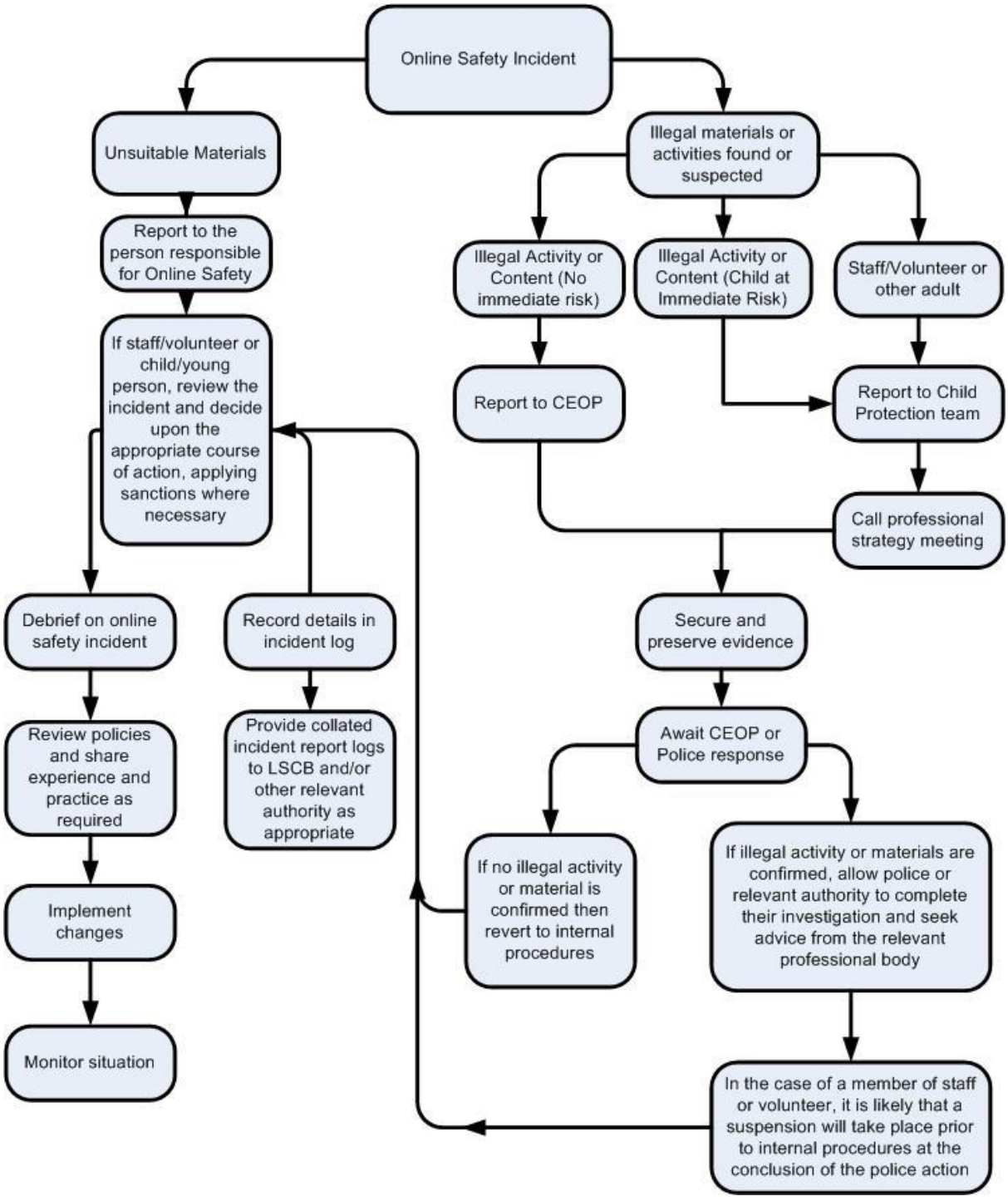
Responding to incidents of misuse

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 (see “User Actions” above).

It is important that staff are aware of the Child Protection and Safeguarding Policy in relation to Child Abuse, in particular sections 24-30, as these are the sections which outline what staff should look out for in lessons and procedures to follow in extreme circumstances.

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.


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

Incidents requiring investigation

It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow school 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 in investigation:

- 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 as outlined in the Child Protection and Safeguarding Policy and the Myton Behaviour Policy.
    - Involvement by Local Authority or national / local organisation (as relevant).
    - Police involvement and/or action
- If content being reviewed includes images of child abuse then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:
    - incidents of ‘grooming’ behaviour
    - the sending of obscene materials to a child
    - adult material which potentially breaches the Obscene Publications Act
    - criminally racist material
    - promotion of 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 school and possibly the police and demonstrate that visits to these sites were carried out for safeguarding purposes. The completed form should be retained by the group for evidence and reference purposes.