The Norwood School Online Safety Policy December 2019

Contents

Introduction

As new technologies emerge, the potential benefits to education can be enormous and present powerful learning opportunities for young people. However, online technologies pose some risks and dangers which staff, students and parents need to be aware of to safeguard all within the school community. This policy outlines the school's approach to managing the use of digital technologies for the benefit of all within the school community.

Development, monitoring and review

This online safety policy has been developed by the Online safety lead in consultation with SLT, students and staff. The policy is based on the model and resources from SWGFL. Consultation with staff in school through:

- Faculty meetings
- Heads of Faculty meetings
- Year team meetings
- Student voice
- Student leadership team
- Governor's meetings.

Schedule

This online safety policy was approved by the governors on	December 2019
The implementation of this e-safety policy will be monitored by the:	SLT Online safety lead
Monitoring will take place at regular intervals:	Every term
The Governors will receive updates on the implementation of the e-safety policy (which will include anonymous details of e-safety incidents) at regular intervals:	Annually
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 e-safety or incidents that have taken place. The next anticipated review date will be:	December 2020
Should serious e-safety incidents take place, the following external persons / agencies should be informed:	LA safeguarding officer, Liaison police officer.

Scope of the Policy

This policy applies to all within the school community, including staff, students, volunteers, parents/carers, visitors and anyone else who has access to, and are users of, the school ICT systems both within and out of school.

Roles and Responsibilities

Governors

- Responsible for approving the Online safety policy
- Reviewing its effectiveness
- Receiving information about Online safety incidents and monitoring
- Supporting decisions following from the implementation of the policy by staff.

Head teacher

- Appointing an Online safety lead and ensuring a duty of care in relation to online safety for students and staff
- Review the work of the SLT with responsibility for online safety SLT E-safety coordinator.
- Approve appropriate resourcing for developing technologies and training opportunities.

SLT

- Be aware of procedures to be followed in the event of serious online safety incidents including allegations against students or a member of staff.
- Ensure staff receive appropriate training on online safety
- Ensure a system of monitoring and reviewing and acting on the evidence arising from online safety monitoring.

Online-safety lead

- Takes day to day responsibility for online safety issues in the school and has a leading role in establishing and reviewing Online safety policies.
- Ensures all staff are aware of procedures that need to be followed in the event of an online safety incident taking place.
- Provides training and advice for staff
- Liaises with local authority and any other relevant body
- Liaises with school network manager
- Receives and acts on online monitoring incidents and maintains a log of all incidents
- Presents to governors at appropriate times
- Reports to school leadership team and the head teacher on the outcomes of monitoring.
- Works with other school staff to ensure sanctions are appropriate to the misdemeanour with respect of online behaviours.
- Raises awareness of Safer Internet Day to whole school staff and students
- Provides parents with relevant updates and alerts in relation to online safety.

Network manager

- Ensures the school's infrastructure is secure and not open to misuse and malicious attack.
- That the school is compliant with safety technical requirements and Local authority guidance.
- That users can only access the school's systems through properly enforced password protection policy.
- Keeps up to date with online safety technical information to be able carry out their duty to inform and update others as relevant.
- Ensures remote access to the network is regularly monitored and any misuse is reported to the Head teacher or the school's IT lead.
- Makes sure that monitoring systems are implemented and updated.

Teaching and support staff

- Have an awareness of online safety matters and of the school's current online safety policy and practice.
- Have read, understood and accept the Acceptable use policy
- Report any misuse to the head teacher or Lead online safety member of staff for investigation or action.
- Ensure all digital communications with parents must be on a professional level and must always be on official school systems.
- Online –safety is embedded in the curriculum and other activities
- Ensure students understand and follow all acceptable use policies.
- Students have good research skills to avoid plagiarism and uphold copyright regulations.
- Monitor the use of digital technologies, mobile devices and implement current policies with regard to these devices.
- Where internet based lessons are pre-planned, students should be guided to pre-checked sites, and the process are in place for dealing with any unsuitable material.

Designated Child protection officers

- Be trained on online safety issues and be aware of the serious child protection issues arising from:
    - Access to inappropriate materials
    - Inappropriate contact with adults/strangers
    - Potential or actual incidents of grooming
    - Cyber- bullying.

Students

- Use the school digital systems in accordance with the student acceptable use policy
- Have a good understanding of research skills to avoid plagiarism
- Understand the importance of reporting abuse, misuse or access to inappropriate material
- Know and understand policies on the use of mobile devices and digital cameras.
- Understand the importance of good online safety practice when using digital technologies out of school, and realise that the school's online safety policy covers actions out of school if related to their membership of the school.

- Know and understand policies in relation to taking and using images and cyberbullying.
- Recognise that taking and posting of any compromising images or videos of other students or staff on any social media platform will result serious sanctions likely to include all of the following:
  - The loss of social time in school
  - An extended day till 4:30pm
  - Up to 5-day external exclusion

Parents and carers

- Ensure their children understand the need to use the internet in an appropriate way.
- Encourage and promote good online safety practice at home and outside of school.
- Support the school in relation to sanctions applied to misuse or abuse of online technologies.
- Follow school guidelines in relation to:
  - Digital and video images taken in school events
  - Access to parents' sections of websites and student records
  - Their children's personal devices in school.

Policy Statements
Education – Students

Whilst technical solutions such as filtering and monitoring are very important, we consider educating students on the appropriate use of Internet and related technologies as an essential part of our Online safety provision. Students need the guidance and support of school staff to recognise and avoid the risks associated with online activity as well as build the resilience to deal with such risks. Online safety education will be provided in the following ways:
A planned e-safety curriculum as part of ICT and other lessons, which is regularly revisited
Online safety messages reinforced as part of a planned programme of assemblies and tutor time activities
Students taught in all lessons to be critically aware of the content they access on-line and receive guidance to validate the accuracy of information.
Students taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
Staff will act as good role models for in their use of ICT, the Internet and mobile devices.

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 / regulation of the children's on-line behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond. The school with therefore provide information and awareness through:

- Letters, newsletters, web site,
- Parents evenings
- Safer Internet Day
- Reference to the relevant web sites / publications eg www.swgfl.org.uk www.saferinternet.org.uk/ http://www.childnet.com/parents-and-carers

Education and training – Staff

It is essential that all staff receive regular and up to date training on Online safety and understand their responsibilities as outlined in this policy.

The Norwood school will offer training to staff as follows:

- All new staff will receive online safety training as part of their Induction to ensure staff understand this policy and Acceptable Use Agreements.

- Regular up to date whole school training will be provided for all staff.

The online safety lead will receive regular updates through attendance at external training events and reviewing documents released by relevant organisations.

This online safety policy will be discussed in relevant team meetings. Online safety lead will provide appropriate training to staff with particular identified online safety needs.

Technical – infrastructure / equipment, filtering and monitoring

The School has a managed service provider, RM who is fully aware of the school's requirements as regards online safety. The school uses a filtering system and all online activity is monitored by an off-site provider – E-safe. E-safe monitors and reports on any inappropriate use of school computers to the Online safety lead and the head teacher.

- RM maintains the security of the school's technical system
- All users have clearly defined access rights to school systems and devices.
- All users have a username and a secure password (See password policy)
- The master password for the school used by the Network manager must be available to the Head teacher's designated person
- The managed service is responsible for ensuring that software licences are up to date and reconciled with 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
The school has provided enhanced / differentiated user-level filtering which enables teachers and or 6th formers to have different levels of access from lower school students.
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 acceptable use policy is in place regarding the extent of personal use that staff and students are allowed on school devices.

School network password policy

Never tell your password to anybody, do not write down your password or otherwise compromise your password in anyway.

If you forget your password, any member of staff can reset a student password, staff passwords can be reset by contacting the RM Network Admin.

Students Password Policy
The password must be at least 6 characters in length
The password must not contain the student's username of the user's full name
Contain at least 3 of the 4 categories below:
Uppercase letters ABCDEFGHIJKLMNOPQRSTUVWXYZ
Lowercase letters Abcdefghijklmnopqrstuvwxyz
Numbers 0123456789
Symbols e.g. ! $ @ # - (Please do not use the & symbol)
Students will be required to change their password at least once every 365 days.

Staff Password Policy
The password must be at least 8 characters in length
The password must not contain the staff member's username or the user's full name characters
Contain at least 3 of the 4 categories below
Uppercase letters ABCDEFGHIJKLMNOPQRSTUVWXYZ
Lowercase letters abcdefghijklmnopqrstuvwxyz
Numbers 0123456789
Symbols e.g. ! $ @ # - (Please do not use the & symbol)
Staff will be required to change their password at least once every 365 days.

Examples of some good passwords: I'm-7he-be5t!, Tr34$uR3^Hun73r, L10n3lM3ss1!, B4r¢4l0nA!

Examples of some poor passwords:
password1, 1234567, qwerty, football, dragon, elephant2

Use of digital and video images
The development of digital imaging technologies has created significant benefits to learning, allowing staff and students instant use of images that they have recorded themselves or downloaded from the internet. However, all need to be aware of the risks associated with publishing digital images on the internet, e.g. avenues for cyberbullying. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. Employers typically carry out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate students about the risks associated with the taking, use, sharing, publication and distribution of images. In particular, they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- In accordance with guidance from the Information Commissioner's Office, parents/carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published or made publicly available on social networking sites, nor

should parents/carers comment on any activities involving other students in the digital / video images.
- Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital / video images that students are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Students must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include students will be selected carefully and will comply with good practice guidance on the use of such images.
- Students' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Written permission from parents or carers for photographs of students published on the school website covered as part of the AUA signed by parents or carers at the start of the year
- Student's work can only be published with the permission of the student and parents or carers.

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

Communications

Social Media - Protecting Professional Identity

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

- Training to include: acceptable use; social media risks; checking of settings; data protection; reporting issues.
- Clear reporting guidance, including responsibilities, procedures and sanctions

- Risk assessment, including legal risk

Staff should ensure that:

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

Students:

- Students are advised not to initiate friend requests with members of school staff as such social media communication is not permitted.
- Any student who adds posts on staff members' pages or posts any derogatory comments about any member of staff on any website or social media platform will be sanctioned appropriately.

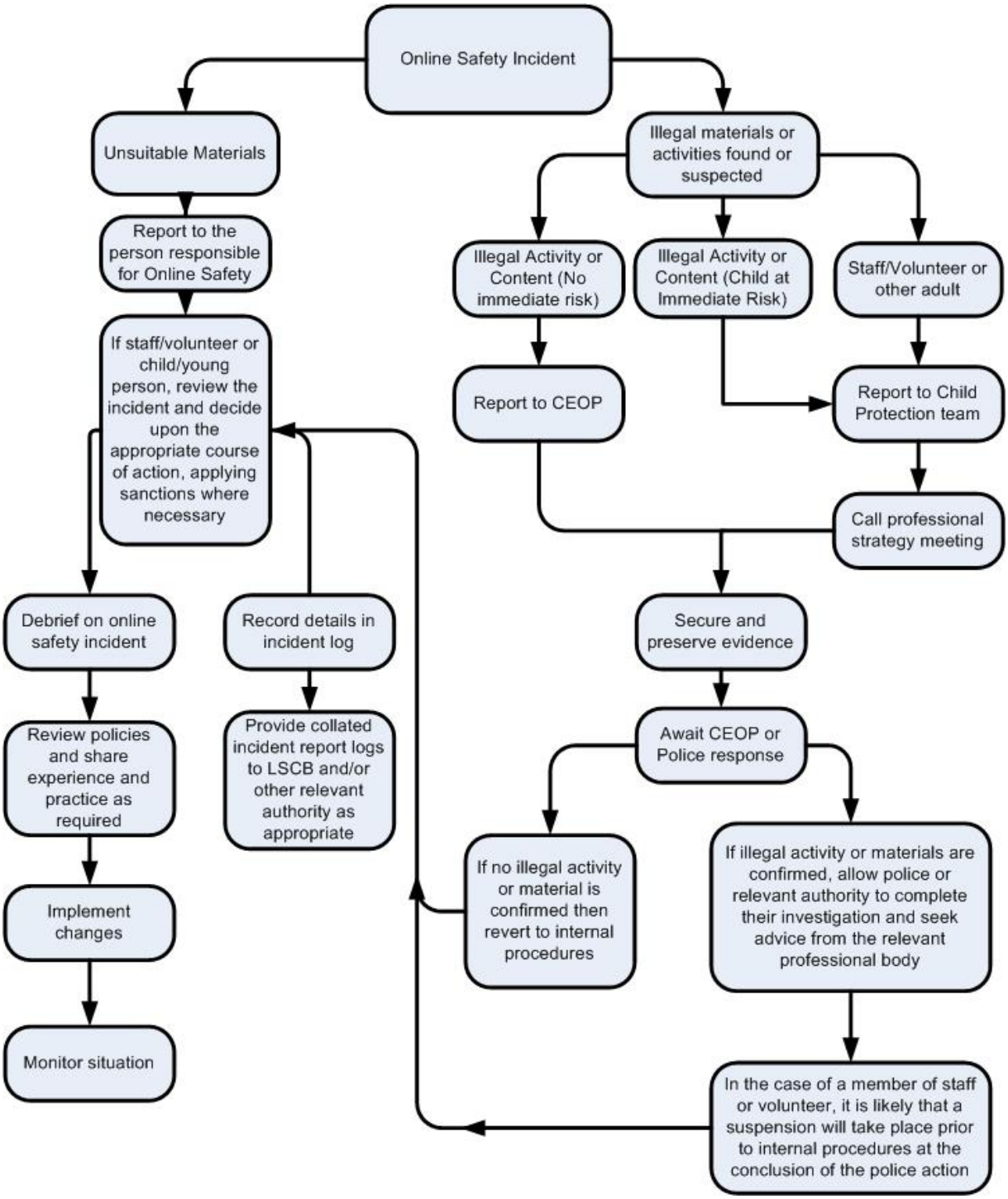
User Actions - unsuitable / inappropriate activities

The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in school or outside school when using school equipment or systems. The school policy restricts usage as follows:

User Actions 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:	Unacceptable	Unacceptable and illegal
Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978		X
Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.		X
Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008		X
criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986		X
pornography	X	
promotion of any kind of discrimination	X	
threatening behaviour, including promotion of physical violence or mental harm	X	
any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute	X	
Using school systems to run a private business	X	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school	X	
Infringing copyright	X	
Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords)	X	
Creating or propagating computer viruses or other harmful files	X	
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)	X	

Responding to incidents of misuse

For incidents which might involve involve illegal or inappropriate activities above, the following flowchart gives a pathway for action.



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.

Other Incidents

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:

Have more than one senior member of staff / volunteer involved in this process. This is vital to protect individuals if accusations are subsequently reported.

Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.

It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).

Record the url of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)

Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:

- Internal response or discipline procedures
- Involvement by Local Authority or national / local organisation (as relevant).
- Police involvement and/or action

- If content being reviewed includes images of Child abuse then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:
  - incidents of 'grooming' behaviour
  - the sending of obscene materials to a child
  - adult material which potentially breaches the Obscene Publications Act
  - criminally racist material
  - other criminal conduct, activity or materials

Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.

It is important that all of the above steps are taken as they will provide an evidence trail for the school and possibly the police and demonstrate that visits to these sites were carried out for child protection purposes. The

completed form should be retained by the group for evidence and reference purposes.

School 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.

Acknowledgement

- This policy is drawn from content from the SWGFL policy template.
- SWGFL, who provide Online safety training for The Norwood School is the leading organisation for Online Safety in the UK.