Torfield and Saxon Mount Academy Trust

Online Safety Policy

(Formerly e-safety policy)

May 2020

Online Safety Policy

Online Safety encompasses Internet technologies and electronic communications such as mobile phones and wireless technology. It highlights the need to educate children and young people about the benefits and risks of using new technology and provides safeguards and awareness for users to enable them to control their online experiences.
The school's Online Safety policy will operate in conjunction with other policies including those concerning pupil behaviour, bullying, curriculum, data protection and security.

Good Habits

Online Safety depends on effective practice at a number of levels:

- Responsible ICT use by all staff and pupils; encouraged by education and made explicit through published policies.
- Sound implementation of Online Safety policy in both administration and curriculum, including secure school network design and use.
- Safe and secure broadband from The Link including the effective management of content filtering.
- Implementation of National statutory standards and specifications.

Contents

School Online Safety Policy

The term 'school' refers to any school within the Trust unless an individual school practice is specified by name.

The school will appoint an Online Safety group. This will be the SLT and may include IT technician staff from time to time for reference.

Our Online Safety Policy has been written by the federation schools. It has been agreed by the senior management team at each school and approved by the Executive Headteacher.

The Online Safety Policy will be reviewed bi-annually. This policy will next be reviewed in May 2021.

Why is Internet use important?

The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management information and administration systems.

Internet use is part of the statutory curriculum and a necessary tool for supporting learning. It is an essential element in 21st century life for education, business and social interaction. Access to the Internet is therefore an entitlement for pupils who show a responsible and mature approach to its use. Our school has a duty to provide pupils with quality Internet access

Pupils will use the Internet outside school and will need to learn how to evaluate Internet information and to take care of their own safety and security.

How does Internet use benefit education?

Benefits of using the Internet in education include:

- Safe access to learning
- Safe access to world-wide educational resources including museums and art galleries
- Safe educational and cultural exchanges between pupils world-wide
- Access to experts in many fields for pupils and staff
- Professional development for staff through access to national developments, educational materials and effective curriculum practice;
- Collaboration across support services and professional associations;
- Improved access to technical support including remote management of networks and automatic system updates;
- Exchange of curriculum and administration data with the Local Authority and DCSF
- Parental access to Academy Website by parents, staff, Trustees and other stakeholders.

How Can Internet Use Enhance Learning?

- The school Internet access will be designed expressly for pupil use and includes filtering appropriate to the age of pupils

- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use
- Internet access will be planned to enrich and extend learning activities.
- Staff should guide pupils in on-line activities that will support learning outcomes planned for the pupils' age and maturity
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation
- Pupils will be educated to safely access carefully planned home learning activities in the event of a school closure (see appendix E)

Authorised Internet Access

- All staff must read and sign the 'Acceptable ICT Use Agreement' before using any school ICT resource. In signing to this, they agree to appropriate use of ICT resources and for the Trust to monitor this
- Parents will be informed that pupils will be provided with supervised Internet access

Internet

- If staff or pupils discover unsuitable sites, the URL (address), time, content must be reported to the Local Authority helpdesk via a senior manager or IT technicians.
- Pupils should be taught to be critically aware of the materials they are shown and how to validate information before accepting its accuracy

Email

- Pupils may only use approved e-mail accounts
- Pupils are encouraged to immediately tell a teacher if they receive offensive e-mail or messaging.
- Pupils are taught to not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission
- Access in school to external personal e-mail accounts using the school network is blocked
- The forwarding of chain letters is not permitted

Social Networking

- The School will block/filter access to social networking sites and newsgroups unless a specific use is approved
- Pupils will be advised never to give out personal details of any kind which may identify them or their location
- Pupils should be advised not to place personal photos on any social network space
- Pupils should be advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications. Pupils should be encouraged to invite known friends only and deny access to others (see also Social Media Policy).

Filtering

- The school will work in partnership with their IT support provider – currently ESCC IT Premier service, and The Link (Internet provision), to ensure filtering systems and firewall are as effective as possible.

Video Conferencing & Skype

- Skype, Microsoft Teams and Video conferencing should use the educational broadband network to ensure quality of service and security rather than the Internet where possible. During COVID restrictions, some pupils are accessing work at home via the internet and Microsoft Teams is the local authority recommended video conferencing application
- Skype or Video conferencing will only be carried out under staff supervision, fully risk assessed and agreed by SLT.

Managing Emerging Technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed
- Mobile phones will not be used for personal use during lessons or formal school time (although use of mobile technology may form part of curriculum provision in which case this will be planned for). The sending of abusive or inappropriate text messages is forbidden

Published Content and the School Web Site

- The contact details on the school website will be the school address, email and telephone number. Staff or pupils' personal information will not be published
- The Executive Headteacher will take overall editorial responsibility for published information on the school website and ensure that content is accurate, relevant and appropriate
- Ensuring the compliance with regulatory authorities' aspect of the school website management is the responsibility of the Executive PA.

Publishing Pupils' Images and Work (See also Policy on the use of Images of Children)

- Photographs that include pupils will be selected carefully and will be appropriate for the context
- Pupils' full names will not be used anywhere on the website
- Written permission from parents or carers will be obtained annually, before photographs of pupils are published on the school website
- Consideration will be given to issues of confidentiality when publishing examples of pupil work

Information System Security

- School ICT systems capacity and security will be reviewed regularly
- Virus protection will be installed and updated regularly

- Staff will be encouraged to change passwords regularly for software that does not have an automatic forced periodic change.
- Security strategies will be discussed with the Local Authority and The Link or any key providers contracted by the academy trust.

Protecting Personal Data

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 and in line with GDPR requirements and legislation. See Data Protection Policy.

Assessing Risks

- The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor ESCC can accept liability for the material accessed, or any consequences of Internet access. The school will audit ICT use to establish if the Online Safety policy is adequate and that the implementation of the Online Safety policy is appropriate.

Handling Online Safety Complaints

- Complaints of Internet misuse will be dealt with by a senior member of staff
- Any complaint about staff misuse must be referred to the Executive Headteacher or Head of School.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures
- Pupils and parents will be informed of the complaints procedure

Communication of Policy

- **Pupils**
  - Rules for Internet access will be posted in the ICT room / Learning resource Centre and all class areas
  - Pupils will be informed that Internet use will be monitored
  - Smoothwall RADAR is in use to constantly monitor all ICT activity
  - The acceptable use agreement is accepted every time a pupil logs onto a computer in school
  - The Education for a Connected World Framework is taught to embed online safety
  - Internet Safety Week events are held annually

- **Staff**
  - All staff will be made aware of the School Online Safety Policy and its importance explained.
  - Staff should be aware that Internet and email traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential
  - Staff that manage filtering systems or monitor ICT use will be supervised by senior management and have clear procedures for reporting issues

- **Parents**

- Parents' attention will be drawn to the School Online Safety Policy in newsletters, the school brochure and on the school website
- Online safety awareness week
- Online safety family learning programme

Appendix A Referral Process

Appendix B Staff Internet Usage

Appendix C Acceptable Use agreement agreed by all staff and pupils

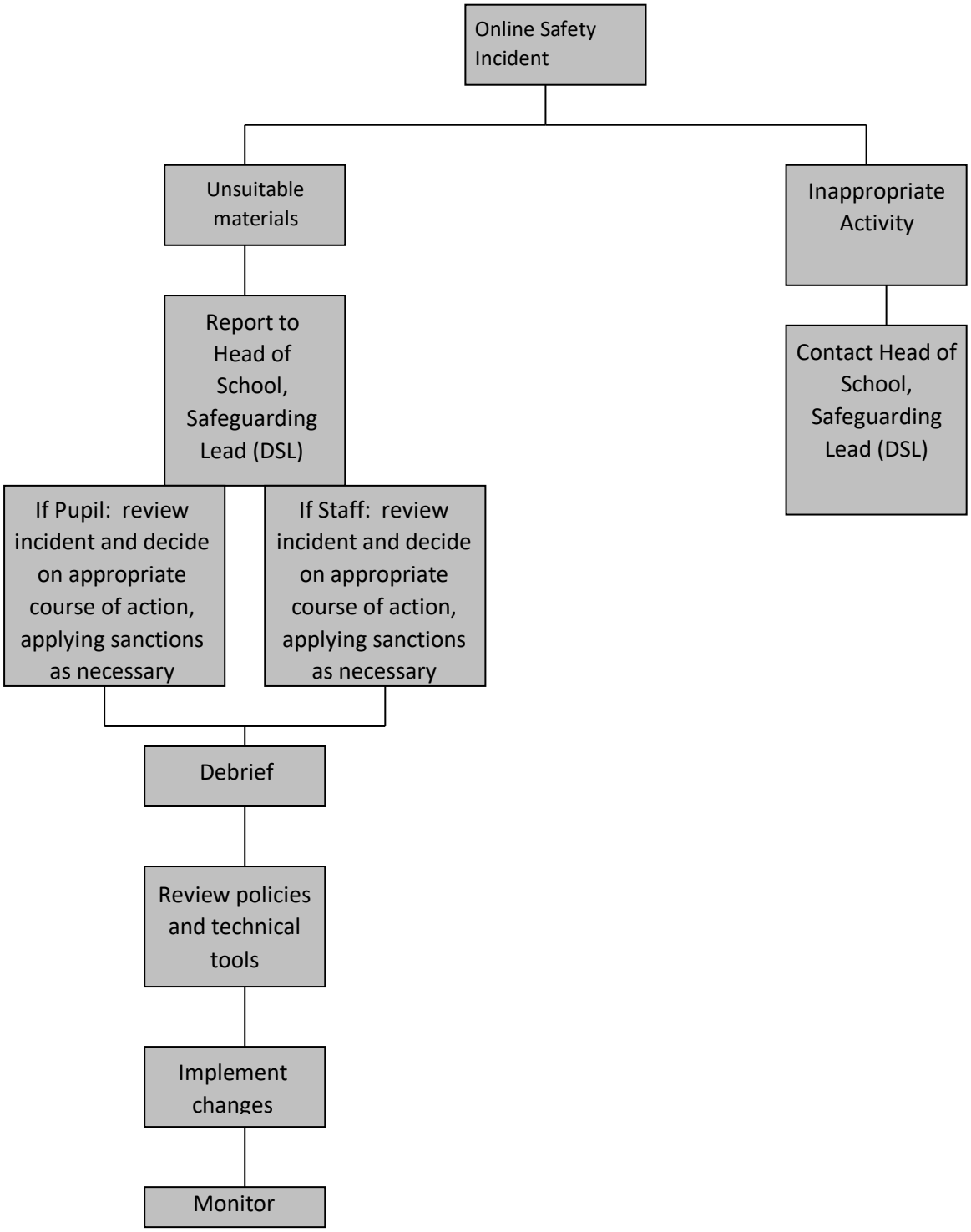
Appendix D Staff Information Systems Code of Conduct

Appendix E Extraordinary Circumstances

Date to be reviewed: May 2022

Appendix A

Flowchart for responding to Online Safety incidents in school



Appendix B

Staff Internet Use Statement

Statement to all staff within the Torfield and Saxon Mount Academy Trust.
This statement is part of a suite of data protection and security documents applicable to all staff in the Trust schools including but not exclusively the Data Protection Policy, Data retention Policy, Electronic Information and Communication policy and Password Policy. All of these must be read in conjunction with this statement and compliance with all aspects understood.

Misuse of Academy Trust Computer Equipment

This statement should be seen as a safeguard for staff and the employer. It applies to all staff working within the Torfield and Saxon Mount Academy Trust, each of whom are required to sign it as an indication that they have read and understood it.

Internet and school data privacy and security

In order to protect security of usage of Trust equipment and identification of users, access user names and passwords must not be shared with or given to any other person under any circumstances. Failure to comply with this will result in disciplinary action and any other measures determined by the Executive Headteacher and Directors as reasonable and appropriate, to protect the assets, reputation and staff and pupils within the Trust schools. Any school equipment taken off site (E.G. a teacher laptop) and /or assigned to an individual member of staff is for that persons use only. No other person is permitted access to school equipment without prior written agreement from a senior manager.

Internet Usage

The internet has become an important research and information tool across the Academy Trust and the proper use of the internet is critical in ensuring a safe and compliant IT environment for staff and pupils.

Accessing inappropriate material will be viewed as a serious disciplinary offence up to dismissal.

Inappropriate material should not knowingly be accessed on any school equipment whether it be in/outside work time or in/outside work premises. This includes portable equipment (i.e. lap-tops).

Inappropriate Materials

Inappropriate materials would cover any materials deemed unsuitable for staff to be accessing in relation to their post within the schools. Examples of such materials are pornographic sites, on-line gambling, extreme political sites, discriminatory sites of any sort (e.g. racist, sexist, ageist, homophobic, disablist. In fact, all sites which conflict with the Academy Trusts equal opportunities policy) or sites which may produce a conflict of interest

(e.g. signing petitions on line which are against school policies/initiatives). This is a non-exhaustive list and should be used to guide staff when considering what sites to access.

It is recognised that staff may be able to access such sites by mistake when using search engines or when firewalls have not been able to prevent it. Where mistakes of this nature occur, staff must immediately notify the Executive Headteacher/ Head of School/ member of the Senior Management Team in writing.

There may be occasions when staff are required to access sites that contain otherwise inappropriate materials in order to carry out their professional duties as determined by the curriculum (e.g. accessing tabloid newspapers and articles about terrorism with regard to a media studies course). Written permission should be sought from the Executive Headteacher/ Head of School, member of the Senior Management Team to search for such sites and, having accessed the sites, a record given to him/her of the material and sites which have been used.

The Executive Headteacher will follow the same procedures outlined above, save that the Chair of Directors is to be consulted and informed.

Personal Use of the Internet

Personal use of school equipment and access to the internet for personal use may be acceptable if used on school premises either before or after normal working hours or in line with school policy standards. Staff need to familiarise themselves with these standards. **The above guidance will still apply during time when the Internet is being accessed for personal use.** Excessive personal use or personal use during working times may lead to disciplinary action.

Monitoring

All Internet use is monitored including personal use.

Employee signature

I confirm that I have read and understood the above statement with regard to using the Internet on School equipment either in or out of the workplace/work time and agree to abide by the terms and conditions of that statement. I am aware that the Academy Trusts security software may record all Internet activity undertaken by me. I am aware that the Trust has a number of Data protection and security related policies and full compliance with these is understood and adhered to. I understand that any violation of the terms and conditions of this statement may lead to disciplinary action.

Signed ……

Date ……

Name (print) ……

School ……

Appendix C

Acceptable Use agreement agreed by all staff and pupils

This computer network has an Acceptable Use Policy (AUP) related to all computer related equipment, network and Internet Use. Any such use which is found to include inappropriate, suggestive, confidential or illegal material to the detriment of its owners or other users and which has been transmitted, received or created on this computer is a violation of the AUP. Any individual found to be in violation of the AUP will be subject to disciplinary action. The computer, related equipment, network and internet is not for personal use. If you do not understand the information in this policy please contact a member of management immediately.

Appendix D

Staff Information Systems Code of Conduct

To ensure that staff are fully aware of their professional responsibilities when using information systems, they are asked to sign this code of conduct. Staff should consult the school's Online Safety policy for further information and clarification.

- The information systems are school property and I understand that it is a criminal offence to use a computer for a purpose not permitted by its owner.
- I will ensure that my information systems use will always be compatible with my professional role.
- I understand that school information systems may not be used for private purposes, without specific permission from the Executive Headteacher.
- I understand that the school may monitor my information systems and Internet use to ensure policy compliance.
- I will respect system security and I will not disclose any password or security information to anyone other than an appropriate system manager.
- I will not install any software or hardware without permission.
- I will ensure that personal data is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely.
- I will respect copyright and intellectual property rights.
- I will report any incidents of concern regarding children's safety to the Designated Safeguarding Lead .
- I will ensure that any electronic communications with pupils are compatible with my professional role.
- I will promote Online Safety with pupils in my care and will help them to develop a responsible attitude to system use and to the content they access or create.
- Failure to comply with school regulations governing ICT usage access may result in disciplinary action being taken.
- Emails should be written applying appropriate professional etiquette
- Staff are responsible for email they send and contacts made
- Use of websites associated with the use of social media e.g. Facebook is prohibited unless directed by the Executive headteacher and as part of DSL role.

- Use of proxy sites is not permitted
- Use of internet is not permitted for private purposes unless agreed by Head of School
- Use of internet for personal financial gain, gambling, political purposes or advertising is not permitted.

The school may exercise its right to monitor the use of the school's information systems, including Internet access, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the school's information system may be taking place, or the system may be being used for criminal purposes, in breach of data protection requirements or for storing unauthorised or unlawful text, imagery or sound.

Appendix E (extraordinary circumstances)

Children and Online Safety away from School

Direct staff and parents to the links provided to the following:

- UK Safer Internet Centre: safe remote learning
- London Grid for Learning: use of videos and livestreaming

The two links above provide some very useful considerations for schools which should be followed when approaching this type of work.

As a starting point you are advised to take heed of the LGfL document which states: There is no expectation that teachers should live stream or provide pre-recorded videos. Schools should consider the approaches that best suit the needs of their pupils and staff. Based upon this you, if you are determined to provide video content, you are advised to consider pre-recorded video rather than live streaming. In the meantime, to support you with your online practice please see the two sets of guidance below:

- ESCC Schools ICT Team have updated their Remote Working Guidance: this includes some technical guidance around distance learning as well as some links to websites.
- On czone you can find a range of digital resources to use with children and young people to promote good mental health within a recently produced document: Digital resources to support mental health.