# Hilltop School

# E-Safety Policy

| | |
|---|---|
| **Date Published** | June 2016 |
| **Version** | 2 |
| **Approved Date** | September 2020 |
| **Review Cycle** | Every 2 years |
| **Review Date** | September 2022 |

"Learning together; to be the best we can be"

## 1. Overview

1.1. Hilltop School is committed to safeguarding and promoting the welfare of children and young people and expects all staff and volunteers to share this commitment. This policy was created by the Safeguarding Team and approved by the Computing Group. This policy will be reviewed annually.

## 2. Introduction

2.1. In today's society, children, young people and adults interact with technologies such as mobile phones, games consoles and the Internet on a daily basis and experience a wide range of opportunities, attitudes and situations. The exchange of ideas, social interaction and learning opportunities involved are greatly beneficial to all, but can occasionally place children, young people and adults in danger.

2.2. E-Safety covers issues relating to children and young people as well as adults and their safe use of the Internet, mobile phones and other electronic communications technologies, both in and out of school. It includes education for all members of the school community on risks and responsibilities and is part of the 'duty of care' which applies to everyone working with children.

2.3. ICT should help all our pupils to develop the skills and capabilities they need to become:

2.3.1. **Successful learners** who enjoy learning, make progress and achieve;
2.3.2. **Confident individuals** who are able to lead safe, healthy and fulfilling lives; and
2.3.3. **Responsible citizens** who make a positive contribution to society.

2.4. As well as being a National Curriculum foundation subject, the ability to use Information and Communications Technology (ICT) effectively is an important life-skill for all our pupils.

## 3. Scope of ICT/E-Safety/Computing

3.1. At Hilltop School, Computing includes the use of any equipment which helps pupils to communicate, use information and control their environment. This includes the use of computers (including the internet), switches,

programmable toys and control kits, assistive technology (specialist key pads, overlay keyboards, touch screens), sensors and probes, electronic musical instruments, audio and video recorders, telephone, digital cameras, scanners and voice activated equipment.

## 4. Benefits of using the Internet in education include:

4.1. access to worldwide educational resources including museums and art galleries;
4.2. educational and cultural exchanges between pupils worldwide;
4.3. access to learning wherever and whenever it's convenient.

## 5. Hilltop Schools' Duty

5.1. The school has a legal duty to ensure that it has done all in its power to protect users of the system and to keep sensitive data safe and secure. This e-Safety policy is an honest attempt to cover all the main areas, and sets out how we plan to develop and establish our e-Safety approach and to identify core principles which all members of the school community need to be aware of and understand.

## 6. Responsibilities:

6.1. Whilst e-safety is the responsibility of the whole school community, the following groups have specific responsibilities:

6.2. **The Local Governing Body** should:

6.2.1. Read, understand, contribute to and promote the school's e-safety policies and guidance;
6.2.2. Understand the benefits and risks of ICT and the internet;
6.2.3. Understand how the school's ICT infrastructure provides safe access to the internet;
6.2.4. Have an overview of how the school encourages pupils to adopt safe and responsible ways of using ICT;
6.2.5. Support the work of the Designated Safeguarding Lead who is responsible for E-Safety in school;
6.2.6. Provide appropriate funding for the implementation of the school's e-safety policy and procedures

6.3. **Senior Leadership Team** should:

6.3.1. Develop and promote an e-safety culture in school.
6.3.2. Support the work of the Designated Safeguarding Lead.
6.3.3. Provide resources, support and training.
6.3.4. Be responsible for the e-safety of the whole school community.
6.3.5. Develop opportunities for learning about e-safety within the curriculum.

6.4. **Designated Safeguarding Lead and Safeguarding Team** should:

6.4.1. Be the first point of contact for e-safety in school.
6.4.2. Develop and maintain e-safety policies and procedures.
6.4.3. Have an understanding of e-safety legislation and guidance.
6.4.4. Promote e-safety to parents, carers and the wider school community.
6.4.5. Develop opportunities for learning about e-safety within the curriculum.
6.4.6. Keep an up-to-date record of e-safety incidents.
6.4.7. Monitor and report on e-safety incidents.
6.4.8. Support SLT in following up e-safety incidents.

6.5. **Computing Subject Leader**

6.6. The Computing Team will:

6.6.1. Promote awareness and a commitment to e-safety throughout school.
6.6.2. Review and approve e-safety policies and procedures.
6.6.3. Have an understanding of E-Safety legislation and guidance.
6.6.4. Provide resources, support and training.
6.6.5. Promote e-safety to parents, carers and the wider school community.
6.6.6. Develop opportunities for learning about e-safety within the curriculum.
6.6.7. Promote new technologies and any identified risks associated across school.
6.6.8. Audit the use of ICT to establish if the e-safety policy is appropriate.
6.6.9. Risk assess any new technology brought into school.

6.7. **Class Teams and Support Teams** should:

6.7.1. Read, understand and help to promote the school's e-safety policies and guidance.

6.7.2. Read, understand and follow the school's Acceptable Use Policy (AUP). (Appendix 2)
6.7.3. Have an understanding of current E-Safety legislation and guidance.
6.7.4. Model safe and responsible use of ICT.
6.7.5. Report all e-safety incidents to the Designated Safeguarding Lead.
6.7.6. Develop opportunities for learning about e-safety within the curriculum.
6.7.7. Carefully supervise pupils' use of ICT in school.
6.7.8. Support pupils to understand the AUP.

6.8. **Technical Support** should:

6.8.1. Read, understand and help to promote the school's e-safety policies and guidance.
6.8.2. Read, understand and follow the school's AUP.
6.8.3. Have an understanding of current e-safety legislation and guidance.
6.8.4. Support the school in providing a safe technical infrastructure to support learning and teaching
6.8.5. Be responsible for the security of the school's ICT systems.
6.8.6. Liaise with the Local Authority, partner organisations and service providers. Model safe and responsible use of ICT.
6.8.7. Report all e-safety incidents to the DSL
6.8.8. To risk assess any new technology, software and apps to be used in school.

6.9. **Pupils** should:

6.9.1. Read, understand and follow the Authorised Use Policy if they are able to.
6.9.2. Help the school to create e-safety policies and guidance.
6.9.3. Learn about the benefits and risks of using ICT the internet and online gaming.
6.9.4. Use ICT and the internet safely in school and at home.
6.9.5. Respect the feelings and rights of other people
6.9.6. Understand what to do if you feel worried, uncomfortable, vulnerable or at risk when using ICT in school or at home
6.9.7. Discuss e-safety in an open and honest way with family and friends

6.10. **Parents and Carers** should:

6.10.1. Help and support the school in promoting e-safety.
6.10.2. Read, understand and promote the school's Authorised Use Policy.

6.10.3. Learn about the benefits and risks of using ICT and the internet.

6.10.4. Discuss e-safety with your children, show interest in how they are using ICT and encourage them to use ICT in a safe and responsible way

6.10.5. Model safe and responsible use of ICT at home

6.10.6. Discuss your child's use of ICT in school

# 7. Learning and Teaching

## 7.1. The importance of Internet Use

7.1.1. Internet use is part of the statutory curriculum and is a necessary tool for learning. The Internet is a part of everyday life for education, business and social interaction.

7.1.2. The school has a duty to provide students with quality Internet access as part of their learning experience.

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

7.1.4. 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 functions.

7.1.5. Internet access is an entitlement for students who show a responsible and mature approach to its use.

7.1.6. Developing good practice in Internet use as a tool for teaching and learning is essential. Respect for copyright and intellectual property rights, and the correct use of published material should be taught.

7.1.7. Whilst the Computing curriculum provides pupils with a whole range of digital skills, because of the cross curricular nature of Internet use, a whole school approach should be adopted.

7.1.8. The school's Internet access will be designed to enhance and extend education and will include filtering appropriate to the age of the pupils via Nexus service filtering system.

7.1.9. Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use through the school curriculum.

7.1.10. All staff will be responsible for reminding pupils of responsible use prior to any Internet session.

7.1.11. Staff should guide pupils to online activities that will support the learning outcomes planned for the pupils' age and ability.

7.1.12. Pupils will be educated in the effective use of the Internet in research.

## 8. Using ICT Safely

8.1. The ability to use ICT safely and responsibly is important for all our pupils. It will help them to safely benefit from the opportunities ICT provides.

## 9. At Hilltop we will

9.1. Promote e-safety through input in morning briefing for staff and whole school activities such as Computing Day

9.2. Provide parents, carers and pupils with relevant e-safety information and updates e.g. the need to protect personal information, consider the consequences of their actions and the need to check the accuracy and validity of information.

9.3. Remind pupils, parents and carers about their responsibilities by asking them to sign an Authorised Use Policy on an annual basis

9.4. Model safe and responsible behaviour in our own use of technology in school.

## 10. Involving Parents and Carers

10.1. It is important to help all our parents and carers to develop the knowledge, skills and understanding they need to keep themselves and their children safe. At Maltby Hilltop we will:

10.1.1. Provide useful links and information on e-safety in newsletters and on the school website;

10.1.2. Provide all parents and carers with links to on-line resources. These will also be available on the school website and Facebook page and is updated when relevant.

10.1.3. Provide information, advice and support through termly Parents and Carers meetings and when issues arise.

## 11. Managing ICT Systems and Access:

11.1. The school will provide safe and secure access to ICT systems.

11.2. All ICT hardware and software will be regularly maintained and updated.

11.3. Virus protection is installed on the school's network. This is activated and kept up-to-date.

11.4. Internet access and levels of internet access are managed by the school.

11.5. All users of ICT will sign up to abide by the Acceptable Use Policy (AUP) on an annual basis.

11.6. Users will be made aware of their responsibility for safe and responsible use of ICT and informed that use of the school's ICT systems is monitored and checked

11.7. All pupils will access the internet using a class log-on

11.8. All pupils, whether supervised or working independently, will follow the school's AUP They should always be monitored to check what material they are accessing. All adults will access the internet using an individual log-on which they will keep secure

11.9. All adults will follow the school's AUP

11.10. Any administrator passwords for the school's ICT systems will be kept secure and available to a minimum of two adults e.g. Office manager and ICT Technician

11.11. The school will take all responsible steps to stop users from accessing inappropriate content. However, it is not possible to guarantee that access to inappropriate content will never happen.

11.12. The school will regularly audit the ICT use and review the effectiveness of E-Safety policies and practice. The school will review internet access provision and consider new methods for identifying, assessing and minimising risks

## 12. Internet Access:

12.1. The school uses a filtered internet service. If a user discovers a website with inappropriate (or potentially illegal) content, this should be reported to the Designated Safeguarding Leader using the appropriate form. The school will report potentially illegal content to the filtering provider, Local Authority and CEOP. The school will regularly review all security systems so that they meet the needs of all users in school.

## 13. Learning Technologies in School:

13.1. Staff and pupils should use approved e-mail accounts which have been allocated by the school. All approved e-mail accounts are monitored and checked. Staff and pupils will be reminded about the need to send polite and responsible messages, about the dangers of revealing personal information, about the dangers of opening e-mails from unknown senders and opening attachments. Communication between staff and pupils and members of the wider school community should be restricted to school matters. Any inappropriate use of the school e-mail system, or the receipt of any inappropriate messages by a user, should be reported to the e-Safety Co-ordinator or the Office manager.

13.2. The school uses Microsoft Teams which has been vetted by Nexus for data privacy and safety. Staff will be reminded about the need to appear professional on these calls in terms of dress and what is said. If another party organises a meeting they might use other communication tools, it can be agreed by the school's data controller but the school cannot guarantee their security. All calls should be logged on CPOMS directly or using the appropriate form. If other students are involved parents must give permission in the same way that permission is given for photos (appendix 8)

13.3. Pupils will be taught about safe and responsible behaviours when creating, using and storing digital images, video and sound. Digital images, video and sound will only be created using equipment provided by the

school. Exceptions will only be made to persons authorised by the Head Teacher upon completion of a signed agreement. Digital images, video and sound will not be created without the permission of participants. Images and video will be of appropriate activities. Full names of participants will not be used either within the material or in any accompanying text. All materials will not be published without the permission of participants or, for pupils, participant's parents and carers. Staff should not use personal devices such as mobile phones or cameras to take photos or videos of pupils and will only use work-provided equipment for this purpose. If personal equipment is used a member of the Senior Leadership Team should be informed and the data downloaded immediately onto school equipment and deleted from the personal equipment. At school events parents/carers will be told not to take pictures/videos so they do not have images of other children.

## 14. Out of School Events

14.1. Parents and Carers of pupils who attend events beyond the normal school day will be notified prior to the event by letter that photographic images and video footage may be taken which will be beyond the school's control.

## 15. Pupils Educated off site:

15.1. Pupils who access part of their learning in another educational establishment require staff to follow the guidance and procedures in line with the school's policy and acceptable use agreement. It is the responsibility of Maltby Hilltop staff members to notify all professionals about the restrictions of publicizing digital images and videos for our pupils.

## 16. Social Networking, Social Media and Personal Publishing:

16.1. Parents and teachers need to be aware that the Internet has emerging online spaces and social networks which allow individuals to publish unmediated content. Social networking sites provide on-line communities and can connect people with similar or even very different interests. Users can be invited to view personal spaces and leave comments, over which there may be limited control. Pupils will not be able to create or post content on websites with public access without adult supervision. Pupils will be taught safe and responsible behaviour in the creation and publishing of online content e.g. pupils will be taught not to reveal personal information.

16.2. Staff and pupils will be encouraged to adopt safe and responsible behaviours in their personal use of blogs and social networking sites. Staff should not have links to school on their personal social media and they are advised to adjust their privacy settings. Staff should not post personal opinions relating to school matters or refer to incidents in school on blogs or social networking sites and staff are strongly advised not to become 'friends' with any pupil, or their parents or carers.

16.3. For responsible adults, social networking sites provide easy to use, free facilities, although advertising often intrudes and some sites may be dubious in content. Pupils should be encouraged to think about the ease of uploading personal information, the associated dangers and the difficulty of removing an inappropriate image or information once published.

16.4. All staff should be aware of the potential risks of using social networking sites or personal publishing either professionally with students or personally. They should be aware of the importance of considering the material they post, ensuring profiles are secured and how publishing unsuitable material may affect their professional status. Staff will be made aware that any conduct that brings the school into disrepute will be regarded as a disciplinary matter.

16.5. The school will control access to social media and social networking sites.

16.6. Staff wishing to use Social Media tools with students as part of the curriculum will risk assess the sites before use and check the sites terms and conditions to ensure the site is age appropriate. The school technician will use the school Risk Assessment checklist. Parents will be informed if appropriate about what information might be shared. Blogs or wikis will be password protected and linked to the school website with approval from the Senior Leadership Team. Members of staff are advised not to run social network spaces for pupil use on an individual basis.

16.7. All members of the school community are advised not to publish specific and detailed private thoughts, especially those that may be considered threatening, hurtful or defamatory. Concerns regarding students' use of social networking, social media and personal publishing sites (in or out of school) will be raised with their parents/carers, particularly when concerning students' underage use of sites. Staff personal use of social networking, social media and personal publishing sites will be discussed as part of staff induction and safe and professional behaviour will be outlined in the school Computer/Internet Use Code of Practice, together with the

potential consequences of unacceptable online behaviour both professional and personal.

16.8. The school is not responsible for issues arising from use of social media/technology outside of school. However, the school does have a duty of care to support parents/students. The school will work with parents if concerns arise.

## 17. Mobile Phones

17.1. Mobile phones will only be used in school with permission from the Class Teacher or Head Teacher. Where staff are required to use a mobile phone for out-of-school or out-of-hours activities, or for contacting pupils or parents, they are encouraged to block their number using 141 at the start of their number. They should only use this for work matters and make sure Senior management are aware if it starts to be used as a form of contact. If the use of a personal device is a necessity then the member of staff should obtain permission from the Head Teacher prior to use and the information logged within the member of staff's HR file. If a member of staff is a personal friend or relation to parent then this should also be logged within the member of staff's HR file Staff will not be expected to use personal mobile phones in any situation where their personal mobile phone number or personal information may be revealed to pupils or parents. Personal mobile phones should not be used to photograph children and young people. Students in post 16 may bring in a mobile at their own risk but they are not permitted to use it during the school day.

## 18. Staff Use of Personal Devices (mobile phones, iPads, tablets)

18.1. Staff are only permitted to use their own personal phones or devices for contacting pupils and their families within or outside of the school in a professional capacity if there is a signed agreement authorised by the Executive Head Teacher or Head of School.

18.2. Mobile phones and devices must be switched off or switched to 'silent' mode, Bluetooth communication should be "hidden" or switched off and mobile phones or devices must not be used during teaching periods or formal school time e.g. Assemblies unless permission has been given by a member of Senior Leadership Team in emergency circumstances.

18.3. If a member of staff is responsible for supervising a student they must not be on their phone, laptop or other device which means they are not giving that child their full attention

18.4. If members of staff have an educational reason to allow pupils to use mobile phones or personal device as part of an educational activity then it will only take place when approved by the Senior Leadership Team and a risk assessment has taken place. Staff should not use personal devices such as mobile phones or cameras to take photos or videos of pupils and will only use work-provided equipment for this purpose. If personal equipment is used a member of the Senior Leadership Team should be informed and the data downloaded immediately onto school equipment and deleted from the personal equipment.

18.5. Staff should not use their own personal devices e.g. laptop, tablet, iPad to deliver lessons or work with pupils, as the school cannot be responsible for the content accessed on such devices.

18.6. Devices loaned to staff by the school e.g. laptops or iPads which are accessed outside of the school network are essentially to support professional activity. These devices are not intended for third party use and members of staff must be aware that they are responsible for the maintenance of confidentiality of school information that may be held on such devices.

18.7. Laptops and other devices loaned to staff are subject to the Laptop/Device Agreement signed by the member of staff.

18.8. All laptops/iPads are 'password' protected. This must not be revealed to pupils or other people.

18.9. If a member of staff breaches the school policy then disciplinary action may be taken.

## 19. Pupil Use of Personal Devices (mobile phones, ipads, tablets):

19.1. Hilltop School strongly advises pupils, parents and carers to not send in and personal devices as the school will not be held liable for any loss or damage.

19.2. Pupils may only use their own device with the permission of the classroom teacher.

19.3. This may be done with permission as a break or as a de-stressing tactic. This should be discussed with parent/carers and agreement made about what how it is being used. (appendix 7).

19.4. No personal information can be used on such a device ie photos taken in school of other pupils

19.5. Mobile phones are not to be used during lesson times unless it is part of the learning activity (e.g. travel training).

19.6. Mobile phones cannot be used at breaks and lunchtimes.

19.7. Pupils are not allowed to take photos of others using their personal device.

19.8. Mobile phones may be confiscated if a pupil does not abide by the school rules.

19.9. Parents could be asked to come and collect these phones.

19.10. Pupils will not be able to access the school internet.

## 20. Visitor Use of Personal Devices (mobile phones, ipads, tablets, laptops)

20.1. All visitors will be informed that taking photographs of pupils is not permitted Parents will be asked to sign an AUP.

20.2. Any breach of this policy will be taken very seriously.

20.3. Any use of the internet by a visitor that is in breach of this policy will be discussed with the visitor. Further action could be taken if the matter is not resolved.

## 21. New Technologies

21.1. New applications are continually being developed based on the Internet, the mobile phone network, wireless, Bluetooth or infrared

connections. Users can be mobile using a phone, games console or personal digital assistant with wireless Internet access. This can offer immense opportunities for learning as well as dangers such as a pupil using a phone to video a teacher's reaction in a difficult situation. The school will keep up-to-date with new technologies and will consider the benefits of these technologies for learning and teaching together with the e-safety risks. The school will review and update the e-Safety Policy in response to any new technologies and their associated e-safety risks

## 22. Protecting Personal Data:

22.1. We will ensure that personal data is recorded, processed, transferred and made available according to the Data Protection Act 2018. Staff will always lock their screen or properly log out from a computer after accessing personal data. Staff will not remove personal or sensitive data from the school premises without the permission of the Head Teacher and without ensuring that this data is kept securely.

## 23. The School Website and Facebook page

23.1. School websites provide opportunities to celebrate pupils' work promote the school and publish resources for projects. Publication of any information online should always be considered from a personal and school security viewpoint. The contact details on the school website will be the school address, email and telephone number. Staff or pupils' personal information must not be published, other than staff name. Subject Leaders will be responsible for ensuring that content relating to their subject areas is accurate, appropriate and up to date. The Executive Head Teacher and Head of School take overall editorial responsibility for online content published by the school and will ensure that content published is accurate and appropriate. The school website will comply with the school's guidelines for publications including respect for intellectual property rights, policies and copyright.

## 24. Publication of Pupil Images and Work

24.1. The security of staff and pupils is paramount. Images or videos that include pupils should be selected carefully and parents/carers permission will be obtained before being electronically published. Pupils' full names will not be used anywhere on the website, particularly in association with photographs without the express permission of parents/carers. Pupils work can only be published with their permission or the parents/carers. Written

consent will be kept by the school where pupils' images are used for publicity purposes, until the image is no longer in use.

24.2. Pupils who are looked after by the authority (LAC) will have not any images published until permission is sought from the leader of the children's disability team.

## 25. Risk Assessment

25.1. As the quantity and breadth of information available through the Internet continues to grow it is not possible to guard against every undesirable situation. Risks can be considerably greater where tools are used which are beyond the schools control such as most popular social media sites. The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer. The school cannot accept liability for the material accessed, or any consequences resulting from Internet use. The school will audit ICT use to establish if the e–Safety policy is adequate and that the implementation of the e–Safety policy is appropriate.

25.2. The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990 and breaches will be reported to relevant authorities. A risk assessment will be carried out before the introduction of any new technology by the ICT Technician.

## 26. Data Protection Act 2018

26.1. In 2018 the Data Protection Act (DPA) was amended to incorporate the principles of the General Data Protection Regulation (GDPR), which was a piece of EU-wide legislation which will determine how people's personal data is processed and kept safe, and the legal rights individuals have in relation to their own data.

26.2. **Main principles**

26.2.1. The amendments to the DPA set out the key principles that all personal data must be processed. Data must be:

26.2.1.1. processed lawfully, fairly and transparently;

26.2.1.2. collected for specific, explicit and legitimate purposes;
26.2.1.3. limited to what is necessary for the purposes for which it is processed;
26.2.1.4. accurate and kept up to date;
26.2.1.5. held securely;
26.2.1.6. only retained for as long as is necessary for the reasons it was collected.

26.2.2. **There are also stronger rights for individuals regarding their own data.** The individual's rights include:

26.2.2.1. to be informed about how their data is used,
26.2.2.2. to have access to their data,
26.2.2.3. to rectify incorrect information,
26.2.2.4. to have their data erased,
26.2.2.5. to restrict how their data is used,
26.2.2.6. to move their data from one organisation to another,
26.2.2.7. and to object to their data being used at all.

26.2.3. **We collect and use personal data in order to meet legal requirements and legitimate interests set out in UK law, including those in relation to the following:**

26.2.3.1. Data Protection Act 2018
26.2.3.2. Education Act 1996
26.2.3.3. Regulation 5 of The Education (Information About Individual Students) (England) Regulations 2013;
26.2.3.4. The Children Act (1989 and 2004)
26.2.3.5. The General Data Protection Regulation (GDPR)

26.2.4. In accordance with the above, the personal data of students and their families is collected and used for the following reasons:

26.2.4.1. To support student learning
26.2.4.2. To monitor and report on student progress
26.2.4.3. To provide appropriate pastoral care
26.2.4.4. To assess the quality of our service
26.2.4.5. To comply with the law regarding data sharing

26.3. Hilltop school will ensure information governance is exercised in line with the law, as outlined in the Nexus MAT Information Governance Policy.

## 27. Responding to Incidents of Concern

27.1. Where there is cause for concern or fear that illegal activity has taken place or is taking place involving the use of computer equipment, the level of response necessary will be determined for the offence disclosed e.g. involving the police. All members of the school community will be informed about the procedure for reporting e-Safety concerns (such as breaches of filtering, cyberbullying, illegal content etc.). The Designated Safeguarding Lead will record all reported incidents and actions taken in the School e-Safety incident log and in any other relevant areas e.g. Bullying or Child Protection log. The Designated Safeguarding Lead must be informed of any e-Safety incidents involving Child Protection concerns, which will then be escalated appropriately. The school will inform parents/carers of any incidents of concerns as and when required. After any investigations are completed, the school will debrief, identify lessons learnt and implement any changes required. Where there is cause for concern or fear that illegal activity has taken place or is taking place the school will contact the relevant authorities and escalate the concern to the Police. All concerns and actions are logged on CPOMS.

27.2. If an incident of concern relating to child protection needs to be passed beyond the school then the Designated Safeguarding Lead will escalate the concern to the Local Authority.

## 28. Handling e-Safety complaints

28.1. Prompt action will be taken if a complaint regarding irresponsible use is made. The facts of the incident or concern will be established and evidence gathered where possible and appropriate. E-Safety incidents may have an impact on pupils, staff and the wider school community both on and off site and can have civil, legal and disciplinary consequences.

28.2. Complaints about irresponsible use must be reported (see appendix 3) to the Designated Safeguarding Lead who will be responsible for handling incidents.

28.3. Any complaint about staff misuse must be referred to the Head of School. Pupils and parents/carers will be informed of the complaints procedure.

28.4. All e–safety complaints and incidents will be recorded by the school, including any actions taken.

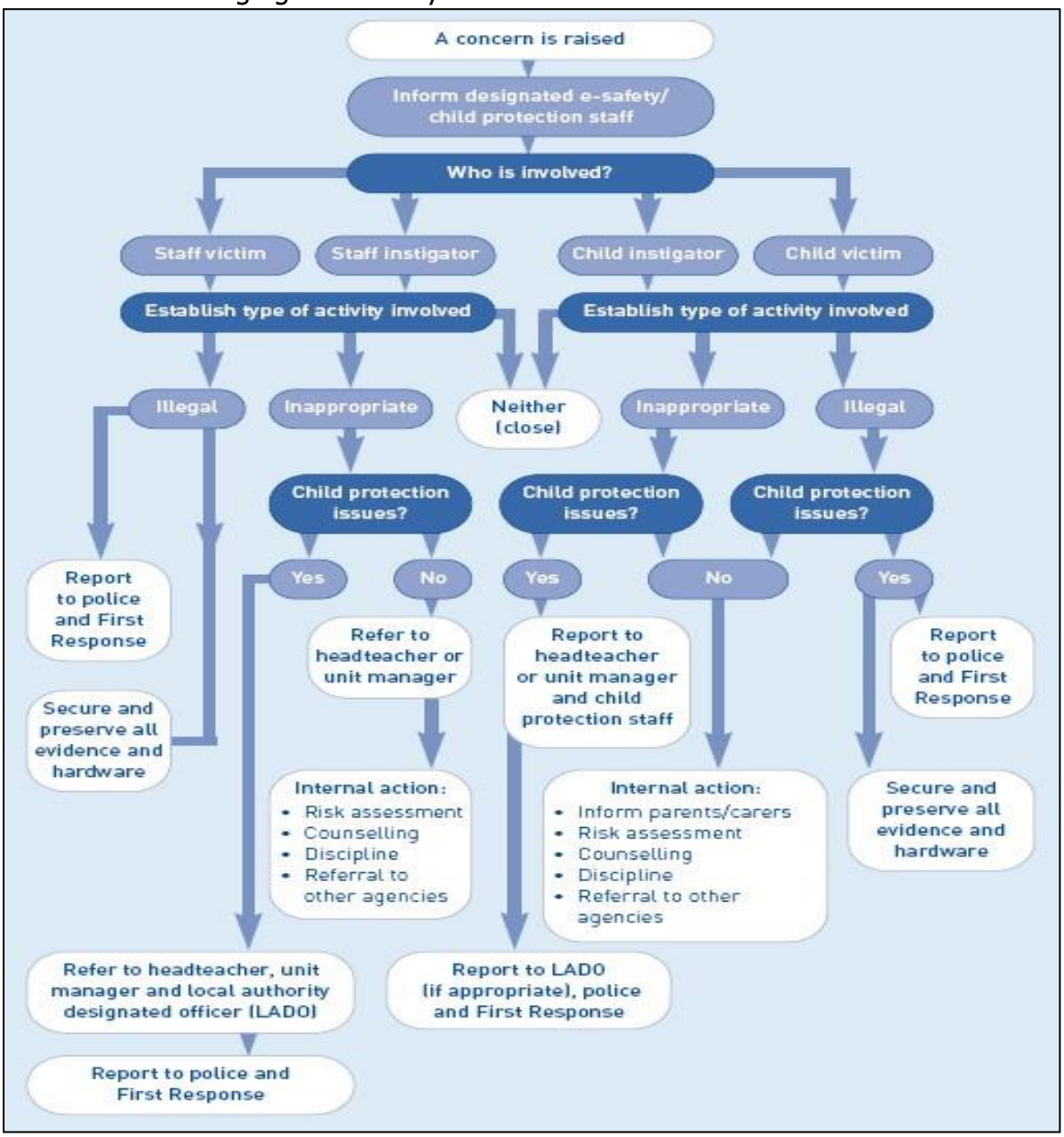
28.5. Parents/Carers and pupils will need to work in partnership with the school to resolve issues.

28.6. All members of the school community should be aware of the importance of confidentiality and the need to follow the official school procedures for reporting concerns. (see appendix 4)

28.7. All members of the school community will be reminded about safe and appropriate behaviour online (in and out of school) and the importance of not posting any content, comments, images or videos online which cause harm, distress or offence to any other members of the school community.

28.8. There may be occasions when the police must be contacted. This is a decision the Head of School or Designated Safeguarding Lead will make when the all the facts are presented.

Flowchart for managing an e-safety incident




## 29. Cyberbullying

29.1. Cyberbullying can be defined as "The use of Information Communication Technology, particularly mobile phones and the internet to deliberately hurt or upset someone" DCSF 2007.

29.2. Many young people and adults find that using the internet and mobile phones is a positive and creative part of their everyday life. Unfortunately, technologies can also be used negatively. When children are the target of bullying via mobiles phones, gaming or the Internet, they can often feel very

alone, particularly if the adults around them do not understand cyberbullying and its effects. A once previously safe and enjoyable environment or activity can become threatening, harmful and a source of anxiety.

29.3. It is essential that our young people, school staff and parents and carers understand how cyberbullying is different from other forms of bullying, how it can affect people and how to respond and combat misuse. Promoting a culture of confident users will support innovation and safety.

29.4. Where bullying outside school (such as online or via text) is reported to the school, it will be investigated and acted on.

29.5. Although bullying in itself is not a specific criminal offence in the UK, it is important to bear in mind that some types of harassing or threatening behaviour or communications could be a criminal offence, for example under the Protection from Harassment Act 1997, the Malicious Communications Act 1988, the Communications Act 2003, and the Public Order Act 1986. If the school feels that an offence may have been committed, advice from the police will be sought.

29.6. DfE and Childnet have produced resources and guidance that can be used to give practical advice and guidance on cyberbullying: http://www.digizen.org/cyberbullying

29.7. Cyberbullying on or off site (along with all other forms of bullying) of any member of the school community will not be tolerated. The school has a comprehensive anti-bullying policy.

29.8. Pupils can report cyberbullying to any of member of staff. The Designated Safeguarding Lead must be informed of any reported cyberbullying so that incidents can be recorded and appropriate procedures followed.

29.9. Staff should report any incidents of cyberbullying they experience to SLT. All incidents of cyberbullying reported to the school will be recorded.

29.10. There are clear procedures in place to support anyone in the school community affected by cyberbullying.

29.11. There are clear procedures in place to investigate incidents or allegations of cyberbullying.

29.12. Pupils, staff and parents/carers will be advised to keep a record of the bullying as evidence.

29.13. The school will take steps to identify the bully, where possible and appropriate. This may include examining school system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police, if necessary.

29.14. Pupils, staff and parents/carers will be required to work with the school to support the approach to cyberbullying and the school's e-Safety ethos.

29.15. Sanctions for those involved in cyberbullying may include:

29.16. The bully will be asked to remove any material deemed to be inappropriate or a service provider may be contacted to remove content if the bully refuses or is unable to delete content.

29.17. Internet access may be suspended at school for the user for a period of time. Other sanctions for pupils and staff may also be used in accordance to the schools antibullying, behaviour policy or Computer/Internet Use Code of Practice.

29.18. Parent/carers of pupils will be informed.

29.19. The Police will be contacted if a criminal offence is suspected.

## 30. Communication Policy

30.1. E-Safety will be introduced and discussed with pupils through the school's curriculum. Posters displaying e-Safety rules are available for display in every classroom. The importance of e-Safety will be reinforced through links to PSHE and cross curricular e-Safety week. Reminders about responsible and safe use should precede lessons where computers and the Internet are being used.

30.2. All users will be informed that network and Internet use will be monitored.

30.3. An e–Safety training programme will be established across the school to raise the awareness and importance of safe and responsible internet use amongst pupils.

30.4. Pupil instruction regarding responsible and safe use will precede Internet access.

30.5. An e–Safety module will be included in the PSHE, Citizenship and/or computing programmes covering both safe school and home use.

30.6. E-Safety rules will be posted in all rooms with Internet access.

30.7. Safe and responsible use of the Internet and technology will be reinforced across the curriculum and subject areas.

30.8. Particular attention to e-Safety education will be given where pupils are considered to be vulnerable.

30.9. The School e–Safety Policy will only be effective if all staff subscribe to its values and methods.

30.10. All staff must understand that the rules for information systems misuse are specific and that instances resulting in disciplinary procedures and dismissal have occurred.

30.10.1. If a member of staff is concerned about any aspect of their ICT or internet use either on or off site, they should discuss this with their line manager or e-Safety coordinator to avoid any possible misunderstanding.

## 31. Admissions

31.1. The importance of online safety will be covered as part of the school's admissions meeting. The pupils AUP and Parent and Carer ICT and e-safety agreement will be included in the pack.

## 32. Parental Support

32.1. Internet use in pupils' homes is increasing rapidly, encouraged by low cost access and developments in mobile technology. Unless parents are aware of the dangers, pupils may have unrestricted and unsupervised access to the Internet in the home. Parent's will be advised of the importance of e-Safety and of suitably, helpful organisations.

32.2. Parents' attention will be drawn to the school e–Safety Policy in newsletters, the school prospectus, on the school website.

32.3. A partnership approach to e-Safety at home and at school with parents will be encouraged. This may include offering parent & carer workshops with demonstrations and suggestions for safe home Internet use, or highlighting e–Safety at other attended events e.g. parent & carers day and sports days.

32.4. Parents & carers will be requested to sign an e–Safety/Internet agreement as part of the Home School Agreement (see appendix 5)

32.5. Parents & carers will be encouraged to read the school Code of Practice for pupils and discuss its implications with their children.

32.6. Information and guidance for parents & carers on e–Safety will be made available to parents.

32.7. Interested parents & carers can contact the school if they require further help and support.

## 33. Communication of Policy

### 33.1. Pupils:

- Rules for Internet access will be posted in all networked rooms. As appropriate to the students
- Pupils will be informed that Internet use will be monitored.

### 33.2. Staff:

- All staff will be given the School e-safety Policy and its importance explained.
- E-safety issues will be done as part of Back to Basics training
- Staff will be made aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Teachers will sign a yearly Nexus AUP which requires them to read different elements of e-safety

### 33.3. Parents:

- Parents' attention will be drawn to the School E-Safety Policy in newsletters, the school brochure and on the school web-site.

## APPENDIX 1

### E-Safety Contacts and References

CEOP (Child Exploitation and Online Protection Centre): www.ceop.police.uk
Childline: www.childline.org.uk
Childnet: www.childnet.com
Children's Safeguards Team: www.kenttrustweb.org.uk?safeguards
Click Clever Click Safe Campaign: http://clickcleverclicksafe.direct.gov.uk
Cybermentors: www.cybermentors.org.uk
Digizen: www.digizen.org.uk
Internet Watch Foundation (IWF): www.iwf.org.uk
Kidsmart: www.kidsmart.org.uk
NSPCC: www.nspcc.org.uk
Safer Interent: www.Saferinternet.org.uk
Teach Today: http://en.teachtoday.eu
Think U Know website: www.thinkuknow.co.uk
Virtual Global Taskforce — Report Abuse: www.virtualglobaltaskforce.com Information Commissioner's Office – Data Protection: www.ico.gov.uk/

**APPENDIX 2**

Computing Acceptable Use Policy (AUP):

This policy is designed to make all adults aware of their responsibilities when using any form of ICT in school.

- I will only use ICT and any related technologies for professional purposes or for uses deemed 'reasonable' by the school.
- I will comply with ICT security policies and not disclose any passwords provided to me by the school.
- I will ensure that all electronic communications with children, young people and adults are appropriate to my professional role.
- I will not give out my own personal details, such as a mobile phone number and personal e-mail address to children and young people.
- I will only use approved e-mail system(s) for work.
- I will ensure that personal data is kept secure and is used appropriately, whether in school, taken off-site or accessed remotely. Personal data can only be taken off-site or accessed remotely when authorised by the school.
- I will not install or use any ICT hardware of software without prior permission.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Images of children and young people will only be taken, stored on the school network and used for professional purposes in line with the school's e-safety policy.
- I understand that all my use of the internet and other related technologies can be monitored and can be made available, on request, to the school.
- I will respect copyright and intellectual property rights.
- I will ensure that my on-line activity, both work-related and in private environments, will adhere to this policy and will not bring my professional role into disrepute.
- I will support and promote the Acceptable Use Policy (AUP) and help children, young people and adults to be safe and responsible in their use of ICT and related technologies

Signed: . . . . . Date: . . . . . .

Name: . . . . . Job Title: . . . . . .

**APPENDIX 3**

Dear Parents and Carers

**Re: Computers and the Internet**

Computers, the internet and lots of other technologies have become an important part of learning in schools. We expect all children and young people to use computers and the internet in a safe and responsible way. We think it is important that all children and young people know how to stay safe when they use computers in school and at home.

I would be grateful if you would read the attached 'ICT Rules' and keep a copy for future reference. If your son or daughter uses a computer or the internet independently we would like you to discuss the rules and, if possible, follow them at home. You can find out lots more about using ICT safely at home on the Government's Childnet KnowITAll website www.childnet-int.org/kia/parents.

If you would like any other advice or information about the ICT rules or E-Safety in general please contact your child's Class Teacher.

Please sign and return the attached form to school

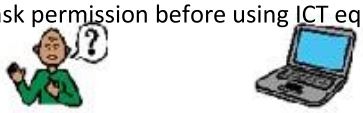
Yours sincerely

David Burdett
Head Teacher

## APPENDIX 4

# ICT Rules

We always ask permission before using ICT equipment:



We keep our passwords a secret:

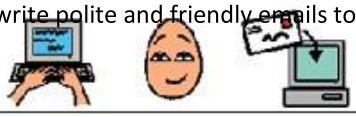
We only ever log onto a computer as ourselves:

We never give out our names, phone numbers or home address to anyone:

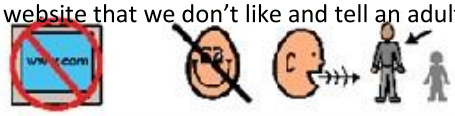
We never arrange to meet someone we don't know:

We only use websites that an adult has chosen or knows about:

We always write polite and friendly emails to people that we know:



We close any website that we don't like and tell an adult:



We never open emails from anyone we don't know:

We know who to ask for help if we are not sure about anything:

Follow these rules to keep safe!

**APPENDIX 5**

## E-Safety Incident Log:

**Please circle the correct issue:** Possible Cause for Concern Accident Near miss

**Name of person (s):** **Date of issue:** / /

**Time of issue:** AM/PM

**Was there a Witness?:** Name: Their role:

**Description of the Concern/Accident/Near miss:**

**Parents were contacted: Yes/No via- Phone call diary face to face other……**

**Has a reason or an account been given? If so please state:**

**Who gave this account?**.....

1. **Details of injury (including location on body)**…… **Please attach body map**
2. **What treatment, if any, was administered?** ……
3. **Was hospital treatment needed?** YES/NO
4. **Was a parent/guardian contacted?** YES/NO Via ……
5. **Did they attend school or hospital?** YES/NO

**Actions taken (including any medical treatment):**

**Reported by :** **Signature:** **Date** /
/

**APPENDIX 6**

# Nexus Trust Acceptable ICT Use Agreement (AUA) and E-Safeguarding Standards

## Introduction

1.1. This Acceptable use policy and conduct agreement addresses the use of electronic communications and will apply to all appointee's deployed by the Trust and provided with authorised access to the Trust's equipment, systems or information. In addition, this document addresses E-Safeguarding standards and expectations.

*Appointee's by definition would include employees and governors of Nexus Multi Academy Trust, Trust board directors and members, consultants, contractors and agents.

1.2. It is the responsibility of every appointee, including those of external and voluntary roles to:

- Read and comply with the requirements of the policy and its appendices.
- Report any breaches of this code e.g. misuse of e-mail, Internet, Intranet, telephones etc. either to their Head teacher/line manager or via the Trust's Confidential Reporting Code.

1.3 This policy can be made available in other languages and formats on request.

1.4 Every appointee has a duty of care for equipment such as phones and computers that are provided for their use. It is expected that appointees will take reasonable steps to maintain the security and safety of equipment. This includes not leaving equipment in view in unattended vehicles and storing it securely when not in use. Mobile phones must be secured by a PIN number to prevent unauthorised use if they are lost or stolen, the PIN number must not be written down or kept with the phone. The loss, damage or malfunctioning of any computer equipment or data storage device must be reported to the school or Trust ICT personnel and Head Teacher.

1.5 Misuse or loss of communications equipment due to negligence will result in appointees being requested to reimburse costs to the Trust and may result in disciplinary action.

### Associated Documents

2.1 Whilst using the Trust's communications technology systems appointees should also ensure they comply with the associated Trust policies on Information Governance and Information Security.

2.2. Reading confirmation checklist (available in hard copy, email or via the trusts website http://nexusmat.org/index.php/about-nexus/policies-and-procedures under "Information Governance")

| | | | |
|---|---|---|---|
| | A. Confidentiality & Sharing Information Policy. | | E. Information Security Incident Reporting Policy. |
| | B. Data Protection Policy Statement. | | F. Information Security Policy. |
| | C. Electronic Communications Policy. | | G. Screen, Assess Plan Procedure Guidance – (Applicable for Trust ELT, LGB, School SLT). |

| | | | |
|---|---|---|---|
| | D. Information Governance Data Protection & FOI Policy. | | H. Employee code of conduct. |

## Key Highlights

- I have read and understood the implications and my personal responsibilities in relation to the use of ICT equipment and systems detailed within this policy and associated documents.

- I will ensure that I am aware of my individual responsibilities relating to the safeguarding of children within the context of E-Safeguarding and know what to do in the event of misuse of technology by any member of the school community.

- I understand that my files, communications and internet activity may be monitored and checked at all times to protect my own and others' safety, and action may be taken if deemed necessary to safeguard myself or others.

- I understand that if I do not follow all statements in this AUA and in other school policies relating to the use of ICT equipment I may be subject to disciplinary action in line with the Trust and or the schools established disciplinary procedures.

## Agreement

**Part A – To be filled in by the Induction Lead/Line Manager**
I can confirm that the information in this document has been discussed in full and that any questions have been addressed.

Print name: …… Position:
……

Signature: …… Date:
……..

**Part B – To be filled in by the Individual**
I can confirm that I have read and understood the content of this document and the associated documents relating to my usage of ICT while carrying out duties on behalf of the trust, act in accordance of the Employee code of conduct policy and maintain the reputation of the Nexus Multi academy Trust.

Print name: …… Position:
……

Signature: …… Date:
……..

**APPENDIX 7**

# E-Safety Contract

I am allowed to use these sites:

I can use the internet to look for

If I do not follow these rules I will not be allowed to use the computer or ipad

Signed:

# APPENDIX 8

Dear Parents/ Carers

The use of video conferencing can be a useful way of holding meetings in the current climate. School might use this service to hold meetings with parents, students, external organisations. If a meeting occurs in class your child must have provided permission even if they are in the background.

The school uses Microsoft Teams which has been vetted by Nexus for data privacy and safety. If another party organises a meeting they might use other communication tools and school cannot guarantee their security.

Parents/guardians should be mindful about what family activities would potentially be heard/seen during the use of video conferencing.

Please dress appropriately when video conferencing and be aware of personal things in the background you might want to keep private such as photographs.

Meetings will not be recorded in any way by anyone taking part in the meeting unless permission has been given by all parties.

As with all communications anything discussed over video conferencing is regarded as confidential and will only be shared with relevant professional bodies that all parties will be made aware of.

Under an UK law called the Data Protection Act 2018, in order for your child to use video conferencing, the school must get your consent.

---

**Please sign below and return the form.**

I understand and accept the use of video conferences in school.

I give/ do not consent for my child, listed below, to use Microsoft Teams.

Student Name: _____

Parent / Carer Printed Name: _____

Parent / Carer Signature: _____ Date: _____

## APPENDIX 9

Please complete and return to school

**Re: Computers and the Internet**

I have: ☐ Read the school's Computing Rules

☐ Discussed safe and responsible use of ICT with my son/daughter

Print Name: .....

Print Pupil's Name: .....

Signed:
.....

Date: .....