Orbis Education Trust

Optimism Resilience Balance Individuality Synergy

Policy Name:	E-Safety and Acceptable Use Policy
Policy Type:	Discretionary
Issue Date:	November 2024
To Be Reviewed:	Biannually - November 2026
Policy Owner:	Mark Wilson

Glossary of Abbreviations and Acronyms used in this Policy

Child Exploitation and Online Protection	-	CEOP.
Designated Safeguarding Lead	-	DSL.
Information and Communications Technology	-	ICT.
Individual Education Plan	-	IEP.
Senior Leadership Team	-	SLT.

INTRODUCTION

1. ICT and the internet have become integral to teaching and learning within schools; providing students and staff with opportunities to improve understanding, access online resources and communicate with the world all - at the touch of a button. At present, the internet based technologies used extensively by young people in both home and school environments include:

a. Websites
b. Social Media
c. Web enables mobile/smart phones
d. Online gaming
e. Learning platforms and Virtual Learning Environments
f. Video broadcasting
g. Blogs
h. Email, Instant messaging and chat rooms colour

2. Whilst this technology has many benefits for our school communities, we recognise that clear procedures for appropriate use and education for staff and students about online behaviours, age restrictions and potential risks are crucial.

3. All schools have a duty to ensure that children and young people are protected from potential harm both within and beyond the school environment. Every effort will be made to safeguard against all risks, however it is likely that we will never be able to completely eliminate them. Any incidents that do arise will be dealt with quickly and according to policy to ensure that children, young people and staff continue to be protected.

AIMS

4. To emphasise the need to educate staff, children and young people about the pros and cons of using new technologies both within, and outside of, the school environment.

5. To provide safeguards and rules for acceptable use to guide all users in their online experiences.

6. To ensure adults are clear about procedures for misuse of any technologies both within and beyond the school or educational setting.

7. To develop links with parents/carers and the wider community ensuring input into policies and procedures with continued awareness of the benefits and potential issues related to technologies.

SCOPE OF POLICY

8. This policy applies to all staff, students, governors, visitors and contractors accessing the internet or using technological devices on trust premises. This includes staff or student use of personal devices, such as mobile phones or iPads which are brought onto our school grounds. This policy is also applicable where staff have been provided with trust issued devices for use off-site, such as a work laptop or work mobile phone.

STAFF RESPONSIBILITIES

Teaching and Support Staff (including volunteers)

9. All staff have a shared responsibility to ensure that children and young people are able to use the internet and related technologies appropriately and safely as part of the wider duty of care to which all who work in schools are bound.

Executive Director (IT Services)/Technical Staff

10. The Executive Director (IT Services) is responsible for ensuring:

a. that the trust and its schools' ICT infrastructure is secure and not open to misuse or malicious attack.
b. that anti-virus software is installed and maintained on trust devices where applicable.
c. that appropriate filtering policies are applied and updated on a regular basis and that responsibility for their implementation is shared with the Designated Safeguarding Leads (DSLs).
d. that any problems or faults relating to filtering are reported to the appropriate DSL and to the broadband provider immediately and recorded on the E-Safety Incident Log.
e. that he/she keeps up to date with E-Safety technical information in order to maintain the security of the trust networks and safeguard children and young people.
f. that the use of the trust networks is regularly monitored in order that any deliberate or accidental misuse can be reported to the DSL and/or the Headteacher of a school, and/or the CEO of the trust.

Children and Young People

11. Children and young people are responsible for:

a. reading, agreeing to, and abiding by, the 'Acceptable Use Rules for Students' *(Appendix B)*.
b. using the internet and technologies in a safe and responsible manner within school.

c. informing staff of any inappropriate materials, cyberbullying or contact from unknown sources (age dependant).
d. actively participating in the development and annual review of the 'Acceptable Use Rules' *(Appendix B)*.

INCIDENT REPORTING

12. In the event of misuse by staff or students, including use of the trust networks in an illegal, unsuitable or abusive manner, a report must be made to the Headteacher/Executive Director (IT Services) immediately and the 'E-Safety Incident Flowchart' followed *(Appendix A)*. Incidents of Cyber Bullying should be reported in accordance with the School's Anti-Bullying Policy.

13. In the event of minor or accidental misuse, internal investigations should be initiated and disciplinary procedures followed where appropriate. Additionally, all security breaches, lost/stolen equipment or data, unauthorised use or suspected misuse of ICT should be reported immediately to the Executive Director (IT Services) and/or Headteacher.

14. All incidents must be recorded on the E-Safety Incident Log, through the Executive Director (IT Services), to allow for monitoring, auditing and identification of specific concerns or trends.

MONITORING

15. Orbis IT Services staff regularly monitor and record user activity, including any personal use of the school ICT systems (both within and outside of the school environment).

16. Monitoring software is installed on most computer equipment used in our schools, which logs such activity as websites visited, programs used, files printed, etc. Random reviews of these logs are undertaken to ensure that equipment is being used appropriately.

17. The Orbis IT Services staff have the facility to access all files on our school networks and to gain access to all email and other messaging services. In the case of individual staff accounts, these privileges are only used under the direction of the Executive Director (IT Services), other Senior members of the trust, and our school leadership teams.

THE CURRICULUM

Our schools strive to embed E-Safety into all areas of our curriculum and key online safeguarding messages are reinforced wherever ICT is used in learning as follows:

a. A thorough programme of skills and competencies are taught across the different year groups to ensure that students are able to explore how online technologies can be used effectively, but in a safe and responsible manner.
b. Students are made aware of copyright issues, data protection, intellectual property and reliability of information sourced on the internet as part of the E-Safety curriculum.
c. Opportunities for informal discussions with students about online risks and strategies for protecting yourself online are built into our curriculum, to ensure that our students are armed with accurate information.
d. Students, parents/carers and staff are signposted to national and local organisations for further support and advice relating to E-Safety issues, including UK Safer Internet Centre, Childline and CEOP.

STUDENTS WITH ADDITIONAL LEARNING NEEDS

18. Our schools strive to provide access to a broad and balanced curriculum for all learners and recognise the importance of tailoring activities to suit the educational needs of each student. Where a student has specific learning requirements, or poor social understanding, careful consideration is given to the planning and delivery of E-Safety awareness sessions and internet access.

EMAIL USE

Staff

19. The trust provides all staff with a professional email account to use for all school related business, including communications with children, parents and carers. This allows for email content to be monitored and helps to protect staff from the risk of allegations, malicious emails or inappropriate contact with children and their families.

20. Under no circumstances will staff members engage in any personal communications with current, recent former students or any minor outside of authorised school systems.

21. All emails should be professional in tone and checked carefully before sending, just as an official school letter would be.

22. Staff should inform their line manager or the IT Services team if they receive an offensive or inappropriate email via any school systems.

Students

23. The trust provides individual email accounts for students to use as part of their entitlement to understand different ways of communicating and using ICT to share and present information.

24. Students will use their school issued email account for any school related communications, including homework or correspondence with teachers. Email content will be subject to monitoring and filtering for safeguarding purposes.

25. Students will be taught about email safety issues, such as the risk of exposing personal information, opening attachments from unknown sources and the management of inappropriate emails. Students will also be guided in the correct tone to use in email correspondence and regularly reminded of restrictions on abusive or inappropriate content.

Both

26. It is the responsibility of each account holder to keep their password secure and to report any suspected breaches of password security to the Executive Director (IT Services) or IT Services staff. Account holders must never share their password with another user or allow access to their email account without the express permission of the Executive Director (IT Services) or another member of the trust Executive Team.

MANAGING REMOTE ACCESS

27. As technology continues to develop at an exponential rate, schools and their staff are increasingly taking advantage of opportunities for off-site access to the school network and email using remote access facilities. For data security and safeguarding purposes, it is crucial that staff are aware of the following restrictions on use:

a. Only equipment with the appropriate level of security should be used for remote access (i.e. up-to-date anti-virus should be installed and enabled; encryption on any devices where sensitive data is stored or accessed if possible).
b. Log-on information should be confidential and use information that cannot be easily guessed (e.g. date of birth, telephone number, number patterns).
c. For security purposes, network access information should not be written down or stored with the device in case of theft or unauthorised access.
d. Staff should not be accessing school systems, in particular those which contain personal data, via unsecured public Wi-Fi connections, due to inherent security issues these connections have.

INTERNET ACCESS AND AGE APPROPRIATE FILTERING

28. Internet Provider:
Southfield School: **Talk Straight / Schools Broadband**
Kingsthorpe College: **Exa Networks**

29. All students are entitled to safe and secure internet access and schools have a duty to deliver this as part of the learning experience. The trust is responsible for ensuring that the school infrastructure and network is as safe and secure as is reasonably possible and that age appropriate internet filtering is in place to protect young users from inappropriate or harmful online content. To this end, our schools have the following filtering measures in place:

30. Filtering levels are managed and monitored in school via an administration tool/control panel, provided by our broadband supplier, which allows an authorised staff member to quickly allow or block access to a site or specific pages and manage user internet access.

31. Age appropriate content filtering is in place across the school, ensuring that staff and students receive different levels of filtered internet access in line with user requirements (e.g. YouTube at sixth form and staff level but blocked to younger students).

32. All users have unique usernames and passwords to access the school network which ensures that they receive the appropriate level of filtering.

33. In addition to the above, the following safeguards are also in place:

a. Anti-virus and anti-spyware software is used throughout our networks.
b. Firewalls are in place to protect the school networks and the information about children and young people they contain from access by unauthorised users.
c. Encryption codes on wireless systems prevent unauthorised use, and guest access is provided via segregated connections.

Staff

34. Expectations for staff online conduct are the same professional expectations as those offline and are detailed in the staff code of conduct.

35. Staff are expected to preview any websites before use, including those which are recommended to students and parents for homework support.

USE OF SCHOOL AND PERSONAL ICT EQUIPMENT

School ICT Equipment

36. A log of all ICT equipment issued to staff, including serial numbers, is maintained and held by the Orbis IT Services team.

37. Staff should ensure that equipment is secured when not in use (e.g. locking workstations when leaving rooms and ensuring that laptops are returned to locked cupboards when no longer needed).

38. Devices owned by the trust are loaned to staff members as required by their duties, on the understanding that they are treated with care and looked after responsibly. Ownership of any such device remains with the trust.

39. Loss or damage to trust equipment should be reported immediately to the Executive Director (IT Services) *(Appendix C)*.

40. All data residing on the school networks or devices owned by the trust is the property of Orbis Education Trust .

41. Personal data, such as digital photographs and music, should not be stored on trust equipment, and may be subject to periodic deletion as part of our monitoring processes.

42. Whilst the trust performs backups of data residing on our systems, we are not responsible for the loss of such data.

43. Personal ICT equipment, such as laptops or memory sticks, must not be connected to the school network without consent from the Orbis IT Services team.

Mobile/Smart Phones

44. Student use:

a. Some students are permitted mobile phones/devices in school for responsible use outside of lesson times, subject to the mobile phone policy currently in place. Misuse of mobile devices on school grounds will result in the loss of this privilege.
b. If there is reason to suspect that a student's mobile device contains inappropriate, harmful or illegal content, the device will be confiscated and a search conducted by a member of the SLT in line with disciplinary powers awarded to staff in the Education Act 2011. Searches will be conducted in the presence of at least one other SLT member and any actions/findings (including contacting the relevant authorities) recoded in the incident report log. Where evidence of illegal

activity is discovered (e.g. indecent images of young people) the device will be locked in a secure area, parents/carers will be notified and the police contacted immediately. *(Appendix A: E-Safety Incident Flowchart)*.

45. Staff use:

a. Personal mobile phones should only be used on our school sites in such a way that the use does not conflict with staff carrying out their required duties.

Laptops/ iPads

46. Personal use of trust laptops or computing facilities, whilst on school sites, are left to the discretion of the Headteacher and may be permissible if kept to a minimum, used outside of lesson times and does not interfere with an employee's work.

47. Some staff are provided with laptops to allow for trust related work to be completed off site. Personal use of the laptop from home (such as web browsing/online shopping etc) is permitted but should be kept to a minimum and use of the device is strictly restricted to the authorised member of staff only (i.e. not family members).

48. Software and apps should not be installed on trust owned devices without prior permission of the Executive Director (IT Services). Restrictions are usually in place to prevent this, as the trust has a duty to ensure software is licensed appropriately.

49. Staff are aware that all activities carried out on trust devices and systems, both within and outside of the school environment, will be monitored in accordance with this policy.

50. Staff will ensure that trust laptops and other devices are made available as necessary for anti-virus updates, software installations, patches, upgrades or routine monitoring/servicing.

Removable Media (Memory Sticks/USB)

51. Where staff may require removable media to store or access sensitive data (e.g. IEPs, student attainment and assessment data) off site, this use should be kept as minimal as possible to restrict the chance of loss. The use of encrypted memory sticks is enforced for staff.

52. Any passwords used for encrypted memory sticks/or other devices will be remain confidential to the user and shared only with authorised IT personnel for security and monitoring purposes.

PHOTOGRAPHS AND VIDEO

53. Digital photographs and videos are an important part of the learning experience for children and young people and, as such, schools have a responsibility to ensure that they not only educate students about the safe and appropriate use of digital imagery, but also model good practice themselves. To this end, there are strict policies and procedures for staff and students about the use of digital imagery within our schools.

54. Consent will be obtained from parents or carers before photographs or videos of students will be taken or used within the school environment, including the school website or associated marketing material.

55. Permission will be sought from any student or staff member before an image or video is taken and the purpose of the activity and intended use of the image will be made clear.

56. Staff are not permitted to use personal devices, such as cameras, video equipment or camera phones, to take photographs or videos of students. However, in exceptional circumstances, such as equipment shortages, permission may be granted by senior members of staff for use of personal equipment for trust related photographs or videos, provided that the there is an agreed timescale for transfer and deletion of the image from the staff member's device. This permission should be in writing for audit purposes.

57. Where photographs of students are published or displayed (e.g. on our school websites) parental consent must be received.

58. Wherever possible, group shots of students will be taken, as opposed to images of individuals and images should never show young people in compromising situations or inappropriate clothing.

SOCIAL NETWORKS

59. Staff must take care when using social networking websites such as Facebook, Instagram, Snapchat or TikTok, even when such use occurs in their own time using their own computer. Social Networking sites invite users to participate in informal ways that can leave you open to abuse, and often make little or no distinction between adult users and children. Current advice is to change your name on social network sites (e.g. using your middle name instead of surname), making it harder for students to find your account. Friends and family could be told your alias, enabling them to still make contact.

60. You should not allow any student to access personal information you post on a social networking site. In particular:

a. You should not add a student to your 'friends list' or be 'following' them.
b. You are encouraged to set the privacy settings so that personal information is not accessible via a 'Public' setting, but to a 'Friends only' level.
c. You should avoid contacting any student privately via a social networking website, even for school-related purposes.
d. You should take steps to ensure that any person contacting you via a social networking website is who they claim to be, and not an imposter, before allowing them access to your personal information.

61. Staff should also take care when posting to any public website (including online discussion forums or blogs) that their comments do not harm their professional standing or the reputation of the trust or its schools – even if their online activities are entirely unrelated to the trust.

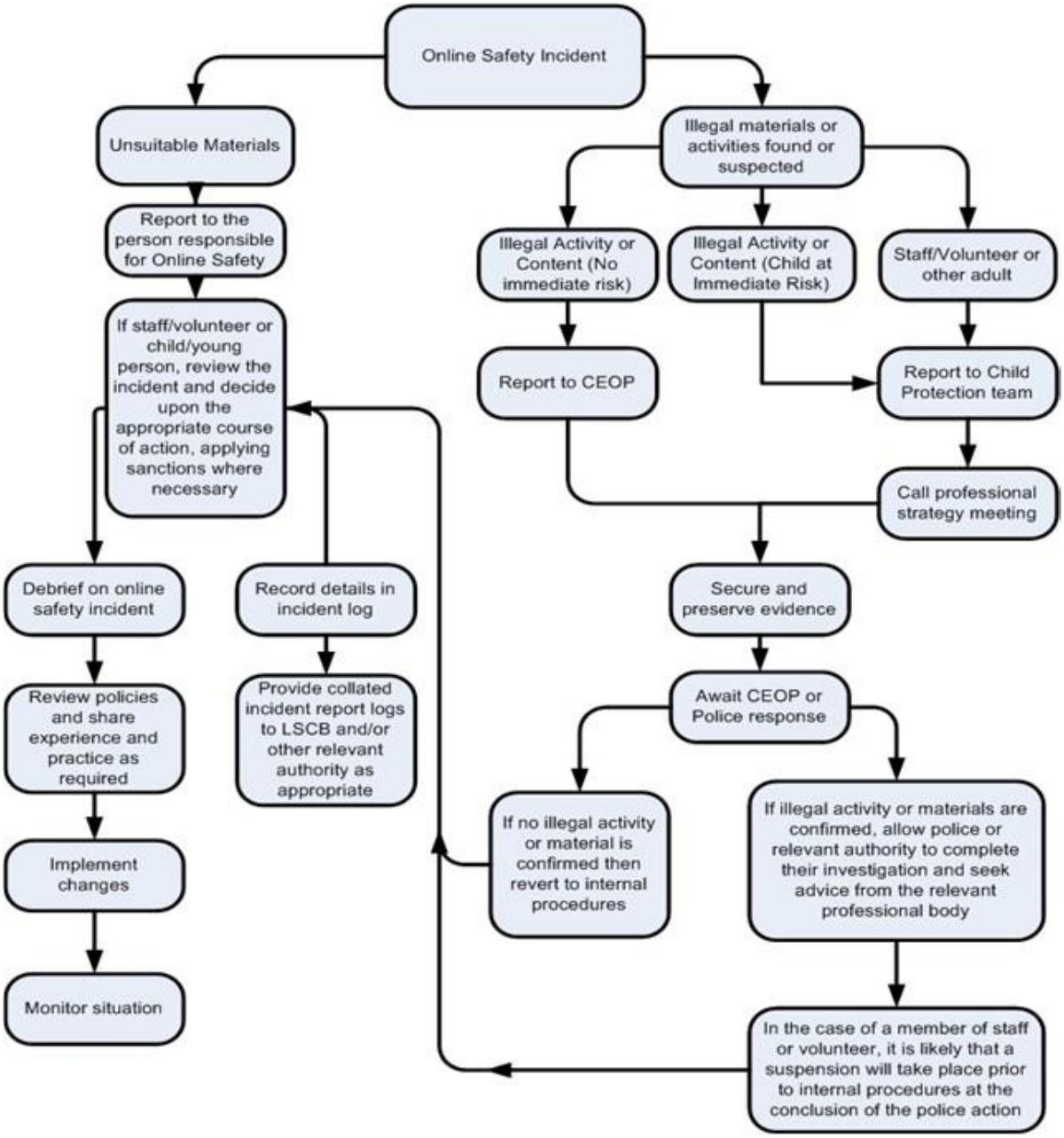
a. Unless authorised to do so, you must not post content on websites that may appear as if you are speaking for the trust or its schools.

b. You should not post any material online that can be clearly linked to the trust or its schools that may damage their reputation.

c. You should avoid posting any material clearly identifying yourself, another member of staff or a student, that could potentially be used to embarrass, harass, or defame the subject.

62. Any concerns, including those about another person, should be raised with the DSL. For further advice, staff are advised to speak to either the IT services team or their union.

APPENDIX A – E-SAFETY INCIDENT FLOWCHART



APPENDIX B - ACCEPTABLE USE RULES FOR STUDENTS

I know that I must use the computers safely

- I know that the school can remotely monitor what I do on the computers.
- I will treat my username and password like my toothbrush – I will not let anyone else use it and I will not use theirs.
- I will be aware of my personal safety when I am communicating online and will not share personal information about myself or others.
- If I arrange to meet someone that I have communicated with online, I will do so in a public place and take an adult with me.
- I will tell a teacher immediately about any unpleasant or inappropriate material or messages on the computer or anything that makes me feel uncomfortable when I see it.
- I understand that the school will look after me and my classmates and can help if anything happens online – even if I am using a computer at home.

I know that I must use the computers responsibly

- I understand that the computers are here for school work and I will only play games on them or use them for personal use if I have permission.
- I will only upload pictures or videos from inside the school if I have permission.
- I understand that the school's security and internet filter is there to protect me, and protect the computer network and I will not try to bypass it. If I need access to a blocked website I will ask my teacher.
- I will only download music or videos onto the computer if it is related to my school work.
- I understand that I must not download or display inappropriate pictures or other material from the Internet.

I know that I must help look after the computers

- If I have a problem with my computer, I will tell a teacher immediately so that the problem can be fixed – I won't leave it broken for the next person.
- I will only use programs that are already on the school computer. If I need a new program, I will ask my teacher - I won't try to install it myself.
- I will not try to connect my own computer or mobile phone to the network.
- I will only change settings on the computer if I am allowed to do so – I won't try to change anything that might cause the computer to go wrong.
- I know that food and drink is not allowed in the computer rooms and that I should not eat or drink around any computer.

I know that I must respect others when using the computers

- I will always treat others the same way I would want them to treat me – just as I would when not using the computers. I will not use the computers to harass or bully anyone.
- I will be polite online and I will not use strong, aggressive or inappropriate language. I appreciate that others may have different opinions.
- I will not take or distribute pictures or videos of anyone without their permission.

APPENDIX C – LIABILITY FOR LOSS OF OR DAMAGE TO SCHOOL EQUIPMENT

Be aware that the school insurance policy does not cover:

- Equipment stolen from unattended cars where the item is not locked in a car boot or glove compartment whilst on school business.
- Equipment stolen where equipment has been left unattended in the open or mislaid.
- Equipment stolen from home whilst in the house or parked vehicle.
- Equipment stolen due to a failure to use adequate security; such as rooms opened by stolen keys or open windows – such thefts are considered to be due to negligence on your part.
- Electrical and mechanical breakdown, maintenance, wear and tear, fraud and dishonesty. Be aware that malicious damage, or damage caused due to negligence, will not be covered.