OAK ACADEMIES TRUST

E-SAFETY POLICY: INCLUDING ACCEPTABLE USE FOR PUPILS AND STAFF

Version	2.0
Approved By	Trust Board – June 2021
Re-issue Date	30 June 2022
Review Date	30 June 2023

REVIEW HISTORY

VERSION NO.	DATE OF CHANGE	CHANGE SUMMARY	REF.
0.2	29.3.21	Branding	
0.3	26.4.22	Added Bring Your Own Device section	
0.3	26.4.22	Comments from DPO	p.14

Table of Contents

1. PURPOSE

1.1 This policy applies to all pupils and staff within the Academy accessing ICT systems both in and out of Trust premises. It also applies to anyone else that accesses Trust ICT equipment, including, but not limited to, volunteers, teaching placements and temporary staff within all Trust premises.

1.2 The Education and Inspections Act 2006 empowers Headteachers, to such extent as it is reasonable, to regulate the behaviour of pupils when they are off Trust premises and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This applies to incidents of cyber-bullying or other e-safety incidents covered by this policy, which may take place out of school, but is linked to membership of any of our schools.

1.3 This policy covers the measures needed by the Trust to address the following matters:

- Responsible ICT use by all staff and pupils
- Compliance with statute
- Duty of care to staff and others whilst using ICT in their work
- Protection of Trust assets such as hardware and software
- Sound implementation of e-safety policy in both administration and curriculum, including secure network design and use
- Protection of the reputation of the Trust and all its schools.

Data will be processed to be in line with the requirements and protections set out in the UK General Data Protection Regulation 2018.

2. OVERVIEW

The Trust is fully committed to ensuring the safety of all those who use its IT equipment. The Internet and other digital and information technologies are powerful tools, which open learning up to new opportunities for everyone. Electronic communications help pupils and teachers to learn from each other. These technologies can stimulate discussion promote creativity and increase awareness of context to promote effective learning.

3. RISKS/DANGERS

The use of new technologies can put young people at risk within and outside the school. Some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to / loss of / sharing of personal information

- The risk of being subject to grooming by those with whom they make contact on the internet.
- The sharing / distribution of personal images without an individual's consent or knowledge
- Inappropriate communication / contact with others, including strangers
- Cyber-bullying
- Access to unsuitable video / internet games
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- The potential for excessive use, which may impact on the social and emotional development and learning of the pupil.

Many of these risks reflect situations in the off-line world and it is essential that this policy is used in conjunction with other school and Trust policies (e.g. Behaviour; Anti Bullying; Child Protection; Curriculum; Data Protection; Information Management; Parental Use of Social Networking and Internet Sites).

As with other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build pupils' resilience to the risk to which they may be exposed, so that they have the confidence and skills to face and deal with them.

4. SECURITY OF ASSETS

4.1 All ICT hardware is the property of the Trust. It has the right of access to all computers and other hardware. This requirement applies to laptops issued to staff for their personal use.

4.2 If the user does not co-operate with such requests, it may be treated as a disciplinary offence.

4.3 All hardware will be clearly marked as the property of the school/Trust and will be invisibly marked to assist with recovery and identification by the police.

4.4 The Network Manager/allocated person will keep an up-to-date record of the items of equipment forming the ICT system. This record may be solely in electronic form.

4.5 No hardware should be removed from a Trust site without written consent from Network Manager/allocated person. Please ask the office staff for clarification.

4.6 A record will be kept of all equipment loaned and returned so that the location is easily traceable. This will be signed and dated by the recipient. Forms/documentation for this purpose will be issued as required.

4.7 When conditions relating to the use and storage of ICT equipment are imposed by insurers, users will be informed. Where failure to follow those requirements leads to loss to the Trust, the user will be held accountable for it.

4.8 Valuable or easily concealed items of equipment will be kept in secure conditions, enclosed, or restrained to provide additional security.

4.9 Only properly licensed software will be used on ICT equipment that is the property of the Trust.

4.10 Original copies of software must be held by the Network Manager/allocated person at each school/site, along with original license documentation.

4.11 Freeware and evaluation copies of software are subject to conditions which must be followed if installed on staff laptops.

5. NETWORK SECURITY

5.1 The Trust recognises that an ICT network that is robust and secure with high levels of availability and resilience is an essential tool in the delivery of high-quality education. It is the prime responsibility of the Network Manager/allocated person within each school to ensure that such a service is available.

5.2 The Network Manager/allocated person within each school will keep an up-to-date record of the users of the ICT system and their access rights. This record may be solely in electronic form.

5.3 Staff members will be made aware of the importance and use of passwords. The Network Manager/allocated person within each school will provide a written guide to staff on how to choose and change their passwords.

5.4 A centrally managed virus protection system will be used on all machines on the network. This system will also apply to laptops issued to staff for their personal use. Such laptops must be connected to the network on a weekly basis to ensure that the protection is up to date.

5.5 Other than on to laptops issued to staff for their personal use, no software may be installed on to the network or computers attached to it. ICT support staff, under the direction of the Network Manager/allocated person at the school, will install and configure software and peripheral devices.

5.6 No changes may be made to the configuration of the network or computers attached to it by staff or pupils.

5.7 Staff may change the configuration of laptops issued for their personal use if agreed in advance with the Network Manager/allocated person at the school.

5.8 A robust backup strategy will be implemented by the Network Manager/allocated person at the school. Backup media will be stored in such a way that a total loss of data and system setup information is impossible.

6. COPYRIGHT AND PLAGIARISM

6.1 The Trust recognises the Copyright, Designs and Patents Act 1988 and will act in accordance with it.

6.2 The Trust recognises that an understanding of Copyright and Plagiarism form an important part of pupils' education.

6.3 All staff are made aware of their responsibilities under the Act as part of their induction training and as necessary in refresher training.

6.4 All staff are responsible for ensuring that all pupils comply with copyright in their work and that the importance of proper attribution is stressed.

6.5 All staff are responsible for ensuring that pupils understand the impact of plagiarism and take steps to prevent it as far as possible.

6.6 Departmental reviews will be used to monitor the conduct of the policy.

6.7 Appropriate licenses will be obtained by the SLT to cover the use of photocopied materials, off air video recordings and others. The conditions of these licenses will be included in the guidance.

6.8 Where staff or pupils wish to use copyright materials as part of their work a request must be made to the copyright holder or their agent. An electronic copy of any request must be retained along with the reply.

7. HEALTH AND SAFETY

7.1 The Trust recognises its responsibilities under the Health and Safety at Work Act 1974 and the need to control the risks associated with the use of ICT equipment and will put in place appropriate measures for eliminating, reducing, and managing them.

7.2 ICT equipment in use within the Trust will be selected on the basis that it is fit for the intended purpose and will be used in accordance with the manufacturers' instructions. Advice of the ICT Network Manager/allocated person must be sought before ICT equipment is procured to ensure compliance with this requirement.

7.3 The H & S Co-coordinator is responsible for the generic risk assessment.

7.4 All staff are made aware of the risk assessment as part of their induction training and as necessary in refresher training. The member of the SLT responsible for Staff Development is responsible for ensuring that the training takes place.

7.5 A comprehensive and robust PAT scheme will be in place to ensure electrical safety.

7.6 Users who fall under the terms of the Display Screen Equipment, Regulations 1992, (Amended 2002) will be entitled to eye tests and protective measures as laid out in the regulations.

7.7 The staff Acceptable Use Policy requires staff who undertake novel work to complete an additional RA.

8. ACCEPTABLE USE: PUPILS AND STAFF

8.1 As with all safeguarding issues, any queries or concerns must be referred to your DSL(s).

8.2 Infrastructure – the network is designed to allow access to resources based on permissions.

8.3 Only authorised users can access the system.

8.4 All users must use a unique username and password to access the system. Advice is given on the best use of passwords. Usernames and passwords are issued by ICT support staff.

8.5 Use of the network is logged.

8.6 Connection to the Internet is using an education specific Internet Service Provider (ISP) who complies with the Department for Education (DfE) standards.

8.7 Additional local filtering of material, along with other technical means is put in place to provide a mechanism to allow appropriate access to resources by individual users.

8.8 The wireless network is configured to prevent access by unauthorised users. Where 3rd party equipment is connected to the network it will be solely on a basis agreed with the Network Manager and generally to allow Internet Access only.

8.9 Remote access to the network is only allowed by existing users utilising secure encrypted technologies.

8.10 The Network Manager is responsible for all the provisions in relation to Network Design and access control.

8.11 The Network Manager is responsible for monitoring the provisions in relation to Network Design and access control and will provide a report to the Head Teacher regarding the adequacy of the arrangements and any breach of security on an annual basis, or as necessary.

9. ACCEPTABLE USE: EDUCATION

9.1 All pupils will be given an appropriate level of knowledge to allow them to develop safe practices in their use of ICT and how to protect themselves from and deal with the effects of cyber bullying (see Anti Bullying policy).

9.2 The Trust recognises that new technologies can transform learning; help to improve outcomes for children and young people and promote creativity.

9.3 As part of achieving this, we aim to create an accessible system, with information and services online, which support personalised learning and choice. However, we realise that it will be necessary for our pupils to have the skills of critical awareness, digital literacy and good online citizenship to enable them to use new technologies safely.

9.4 To this end we will:-

- Provide an age-related, comprehensive curriculum for e-safety which enables pupils to become safe and responsible users of new technologies. This will include teaching pupils to exercise the skills of critical awareness, digital literacy and good online citizenship.

- Audit the training needs of all school staff and provide training to improve their knowledge and expertise in the safe and appropriate use of new technologies.
- Work closely with families to help them ensure that their children use new technologies safely and responsibly both at home and school. We will also provide them with relevant information on our e-safety policies and procedures.

9.5 All staff will receive training in e-safety and cyber bullying as part of their induction and safeguarding training. All staff will receive appropriate refresher training as necessary.

9.6 Opportunities will be taken to incorporate e-safety materials in assemblies, digital signage and other means of raising the importance of this area.

9.7 Incidents of cyber bullying will be regarded as bullying and will be thoroughly investigated as in any other case of bullying, the SLT responsible for Pupil Welfare has oversight of this.

9.8 The full range of sanctions identified in the Behaviour Policy will be available in cases of cyber bullying.

9.9 A log of incidents relating to issues of e-safety with pupils will be kept by the member of the SLT responsible for Pupil Welfare.

9.10 The impact of the e-safety strategy will be monitored by the Leadership team.

9.11 As necessary, the Head teacher will report to Governors and ensure that the School Improvement Plan incorporates appropriate provision for future improvements in practice.

9.12 Advice from specialist bodies such as the Child Sexual Exploitation, PREVENT and On-line Protection (CEOP) will be taken account of in the monitoring of the standard of e-safety and future improvements.

10. ACCEPTABLE USE: PUPILS

The rules below are good advice, if you follow them at home and at school you will keep yourself safe and make sure that the ICT system is safe for others.

10.1 You may only use your own username for access to the system; you must keep your password secret, even from your best friends.

10.2 You must never pretend to be anyone else, not even for a joke.

10.3 When you are using the World Wide Web or e-mail, never disclose your name, address, or phone number to a contact.

10.4 If a contact makes offensive or threatening suggestions break off the contact and report the incident to a teacher.

10.5 In lessons, only use the parts of the system that your teacher tells you. If you wish to use other facilities to extend your work, you must ask first.

10.6 Do not assume that your My Documents folder is secret, other users will not be able to access it, but members of staff can. Regular checks will be made on the content of files and emails.

10.7 Out of lessons you may only use the system when there is a teacher present. Manor High students may also book a machine in the Resource area.

10.8 You must not install any software on the system.

10.9 Users are not allowed to:

• Visit Internet sites, make, post, download, upload or pass on, material, remarks, proposals, or comments that contain or relate to:

- Indecent images of children
- Promoting discrimination of any kind
- Promoting racial or religious hatred
- Promoting illegal acts
- Any other information which may be offensive, embarrassing or upsetting to peers or colleagues (i.e cyberbullying) e.g. abusive text or images; promotion of violence; gambling; criminally racist or religious hatred material.

10.10 If you discover any offensive material whilst you are using the system, you should note the location and report it. As a simple guide ask yourself, "Would I get in trouble if I showed this to Mum or Dad?" If you are not sure, do not do it.

10.11 Incidents which appear to involve deliberate access to websites, newsgroups and online groups that contain the following material will be reported to the Police:

• Images of child abuse (images of children whether they are digital or cartoons, apparently under 16 years old, involved in sexual activity or posed to be sexually provocative)
• Adult material that potentially breaches the Obscene Publications Act in the UK
• Criminally racist or anti-religious material
• Violence and bomb making
• Illegal taking or promotion of drugs
• Software piracy
• Other criminal activity

10.12 You must not make changes to the set-up of hardware and software.

10.13 If you ignore these rules whilst you are using the school system you may have your access to the network withdrawn.

11. ACCEPTABLE USE: STAFF

11.1 Use with Pupils

When staff use ICT with pupils, they need to be aware of their responsibilities; both to ensure that their duty of care to the pupils is fulfilled and that the integrity of the ICT system is maintained. Staff should also be clear that educating pupils in the safe use of ICT is an essential part of every planned ICT activity.

11.1.1 Staff should be familiar with the Acceptable Use Policy for pupils and take action to ensure that pupils follow it.

11.1.2 Staff should be familiar with the Generic Risk Assessment for the classroom use of ICT and ensure that, where relevant, it is followed.

11.1.3 Staff should ensure that if their use of ICT falls outside of the terms of the Generic Risk Assessment, an assessment relating to the activity concerned is undertaken. Advice on RA can be obtained from the Health and Safety coordinator and the ICT support team will advise on specific ICT related issues.

11.1.4 When pupils use ICT, staff must be able to monitor that only appropriate material and programs are used. In general, that means that pupils' work can be readily seen by the teacher.

11.1.5 Should staff discover pupils using inappropriate materials, they should attempt to identify the source of the material and report this to the DSL, network manager and SLT. Recording the username of the pupil and the time of the incident will enable the ICT Support Team to check log files and identify the source of the material. Do not assume that the appearance of inappropriate material is always the result of pupil actions. Use judgement and take the opportunity to ensure that the pupil understands how to keep safe.

11.1.6 Members of staff must not allow pupils to use staff user accounts to access the network.

11.1.7 Members of staff should ensure that confidential material is not displayed to pupils. (This can easily happen when pupil data is being displayed on a computer that is also being used to project teaching materials.)

11.1.8 Where pupils are working collaboratively, staff should arrange for appropriate means of sharing work to be setup. (ICT support can advise in this area.)

11.1.9 Staff need to be alert to the possibility of plagiarism and failure to comply with copyright by pupils. Staff must act to ensure that any breaches are properly dealt with. In most cases a reprimand should be sufficient. However, it should be noted that in some cases breach of copyright is a criminal act. If in doubt, please consult a senior member of staff.

11.2 Use of the Network

11.2.1 Staff are not permitted to install software on the system. This includes system updates, printer drivers and so on. The IT Services Team assumes responsibility for all software installation and upgrades.

11.2.2 Staff are not permitted to install hardware on the system. The IT Services Team assumes responsibility for all software installation and upgrades.

11.2.3 Staff are expected to be exemplary in the way that they care for and use the ICT system.

11.2.4 Staff must not view any material that it would be inappropriate for pupils to use, even if that material is suitable for adults. Examples of such material include pornography, violent material, and racist or sexist images or text.

11.2.5 Should they inadvertently encounter inappropriate materials, staff should endeavour to record the location of it and report the instance to IT Services. If staff are concerned that they have inadvertently accessed material, the possession of which might compromise their professional standing, they are strongly advised to refer the matter to a member of the SLT as soon as is possible. Again, a record of the location or route to the material would be of use to allow the blocking of further access.

11.2.6 Should staff wish to view materials that may be questionable, with a view to using them within a teaching context, this can be done provided a senior member of staff is consulted in advance.

11.2.7 It is likely that such access will be very rare and rigorous precautions will be put in place.

11.2.8 Staff must ensure that they comply with the Copyright, Designs and Patents Act 1988. All images and text on the Internet and within educational material are copyright unless they are clearly marked as not being; they must not be used, even for educational purposes, without permission.

11.2.9 Staff must ensure that they comply with the Computer Misuse Act 1990 and the Police and Justice Act 2006. Both acts make unauthorised access to computer systems illegal.

11.2.10 Staff must ensure that they comply with the UK General Data Protection Regulations 2018 (GDPR).

11.2.11 Staff should use their school e-mail account for all school business. (The school e-mail system is backed up and it is possible for your account to be accessed, for example in the instance of your absence.) Should staff use e- mail to communicate with parents, they should be aware that prompt responses will be expected by parents and if they are going to be unavailable for some time, for example on a trip or absent through illness, an "out of office" reply should be set up or your mail should be redirected to a colleague. ICT Support will assist with this.

11.2.12 Staff should be aware that their e-mail is not routinely monitored. Where serious misconduct is suspected staff e-mail may be read by those with responsibility for investigating the alleged offence. E-mail records would be surrendered to police or other investigative bodies should a legitimate request be made.

11.2.13 The sending or receiving of messages which contain any inappropriate material is strictly forbidden. This material includes, but it not limited to, pornography, unethical or illegal requests, racism, sexism, inappropriate language, or any other use which may be likely to cause offence. Disciplinary action will be taken in all cases.

11.2.14 Should staff use e-mail to communicate with pupils, which is seen as an appropriate educational activity, they must be assiduous in ensuring that all e-mails are entirely appropriate. Never disclose personal contact details since this could be mis-interpreted.

11.2.15 Staff should not use public social networking sites for school business, especially contacting pupils or parents. Suitable facilities for this type of interaction can be provided in a secure and monitored manner. Please see ICT support for further advice.

11.2.16 Protect your work by keeping your password to yourself; never use someone else's logon name or password.

11.2.17 Always be wary about revealing your home address, telephone number or picture to people you meet on the Internet.

11.2.18 Staff My Documents areas are not routinely monitored. However, the school has the technical means and legal authority to do so. This will not take place without informing the member of staff concerned unless serious misconduct is suspected. Police and other investigative bodies would be given access to staff areas were a legitimate request to be made.

11.2.19 The use of school resources for the conduct of business, either on the behalf of a staff member or a third party must not take place.

11.2.20 The use of school resources to produce educational material or other items on which they wish to claim intellectual property rights can result in the school being able to claim rights in such intellectual property.

11.3 Bring Your Own Device Considerations – Staff

The Trust recognises that many staff choose to access school information from their own devices.

Any member of staff wishing to do this must be aware that they have a direct personal responsibility for ensuring that the device they choose to use has the benefit of encryption, that is above and beyond a simple password protection.

Staff must ensure that personal devices such as mobile smart phones, tablets and other portable electronic equipment are set to lock and only open with encrypted passcodes to prevent unauthorised access.

School will support and enable staff to ensure that their devices are compliant.

If any member of staff uses a device without these safeguards in place it will be a disciplinary breach if data is unlawfully accessed by a third party.

Encryption protection will be available for staff and suitable advice provided.

11.4 Use of Staff Laptops

This section relates to laptops and any other item of ICT equipment that is issued to staff for their personal use.

Laptops and other ICT equipment are issued to staff to enable them to be more effective in their role.

With the exceptions listed below, the points listed in "Use of the Network" apply to the use of laptops and other items of ICT equipment.

11.4.1 Changes to set-up and configuration of laptops may be made, providing they can be accomplished with the access rights of the normal user of it. Any changes which prevent the proper operation of the laptop on the network will need to be reversed.

11.4.2 Staff may connect their laptop to alternative ISP and home wireless networks. In some instances, this will not be effective due to restrictions installed on the laptop or due to the configuration by the ISP or of the wireless network. ICT support will offer advice on these issues but cannot guarantee to affect a connection in every case.

11.4.3 Equipment that is loaned to staff on a short-term basis should be signed out either with the Hood concerned or ICT support.

11.4.4 Equipment loaned to staff is insured whilst it is at the home of the member of staff and whilst it is in transit. However, conditions apply, the main ones are as follows:

- Equipment is NOT covered whilst in unattended vehicles.
- Equipment must be stored at least 30 cm above ground level to avoid damage from flood water.
- The first £200 of loss is not covered.

11.4.5 Staff who are concerned or who wish to obtain further details about insurance cover should talk to the Business or Office Manager.

11.4.6 Should equipment be subject to un-insured loss, the school would consider seeking recompense from the member of staff to whom the equipment is loaned.

11.4.7 The user of the equipment is responsible for all personal files and data stored on the equipment. Backup of the data is the responsibility of the user. It is strongly recommended that all data is regularly backed up, either to an encrypted memory stick or to the Trust network. Where removable media is used the user must ensure that these media have not been used to download materials that are at risk of damaging the network. It is recommended that the IT Services team transfers files for users.

12. STANDARDS AND INSPECTION

The Trust recognises the need to regularly review policies and procedures in order to ensure that its practices are effective and that the risks to pupils are minimised.

12.1 Monitoring

12.1.1 Monitoring the safe use of new technologies includes both the personal use of the Internet and electronic mail and the monitoring of patterns and trends of use.

12.1.2 With regard to monitoring trends, within the Trust and individual use by staff and pupils, the Trust will audit the use of the Internet and electronic mail to ensure compliance with this policy. The monitoring practices of the Trust are influenced by a range of national and Local Authority guidance documents and will include the monitoring of content and resources.

12.1.3 We will also monitor the use of mobile technologies by pupils, particularly where these technologies may be used to cause harm to others, e.g., bullying (see anti-bullying policy for further information). We will also ensure that staff understand the need to monitor our pupils, and where necessary, support individual pupils where they have been deliberately or inadvertently subjected to harm.

12.2 Sanctions

12.2.1 We will support pupils and staff as necessary in the event of a policy breach.

12.2.2 Where there is inappropriate or illegal use of new technologies, the following sanctions will be applied:

• **Child / Young Person**

- The child/young person will be disciplined according to the behaviour policy of the school.

- Serious breaches may lead to the incident being reported to the Police or other regulatory bodies, for instance, illegal Internet use or child protection concerns.

• **Adult (Staff and Volunteers)**

- The adult may be subject to the disciplinary process, if it is deemed he/she has breached the policy

- Serious breaches may lead to the incident being reported to the Police or other regulatory bodies, for example, illegal Internet use or child protection concerns.

12.2.3 If inappropriate material is accessed, users are required to immediately report this to the Headteacher or CEO so this can be considered for monitoring purposes.

13. <u>REPORTING ABUSE</u>

13.1.1 There will be occasions when either a pupil or an adult within the Trust receives an abusive email or accidentally accesses a website that contains abusive material. When such a situation occurs, the expectation of the Trust is that the pupil or adult should report the incident immediately.

13.1.2 The Trust also recognises that there will be occasions where pupils will be the victims of inappropriate behaviour that could lead to possible or actual significant harm, in such circumstances current safeguarding procedures should be followed. The response of the Trust will be to take the reporting of such incidents seriously and where judged necessary, the Designated Senior Person for Child Protection within the School will refer details of an incident to Children's Social Care or the Police.

The Trust, as part of its safeguarding duty and responsibilities will assist and provide information and advice in support of child protection enquiries and criminal investigations.

14. WORKING IN PARTNERSHIP WITH PARENTS AND CARERS

14.1 We are committed to working in partnership with parents and carers and understand the key role they play in maintaining the safety of their children, through promoting Internet safety at home and elsewhere.

14.2 We also appreciate that there may be some parents who are concerned about the use of the new technologies in their school. In such circumstances staff will meet with parents and carers to discuss their concerns and agree upon a strategy that will allow their child to fully access the curriculum, whilst remaining safe.

15. GUIDANCE ON COPYRIGHT

Guidance on Copyright for state-funded Primary and Secondary Schools.

Introduction

The Department for Education (DfE) buys copyright licences for all state-funded primary and secondary schools in England – covering schools for almost all their copyright requirements.

Purchasing these licences directly means that DfE can save schools money and the administrative time involved in applying for many different licences.

The licences mean you can copy, re-use and share content from a wide range of sources within your school for non-commercial, educational purposes.

The school leadership (head and chair of governors) needs to make sure that:

- all intended activities are covered adequately by the licences
- all staff follow the terms and conditions

For more information on what content you can use, and how to gain other permissions, contact the relevant organisation from the following list.

The copyright licences cover a range of content from printed materials to radio and TV broadcasts:

- Copyright Licensing Agency, for copying text and still images from most books, journals and magazines plus a range of digital publications
- Printed Music Licencing Ltd provides the Schools Printed Music Licence which allows a copy or arrangement to be made of sheet music from printed music publications. The licence is administered by the Centre for Education and Finance Management (CEFM).
- NLA Media Access, for copying from newspapers and magazines. The Copyright Licensing Agency administers this licence and has information on copying from print and digital newspapers
- Educational Recording Agency, for recording and use of radio and television programmes and clips, including catch-up services like BBC iPlayer, for educational use. The Centre for Education & Finance Management administers this licence and operates a helpdesk for schools providing information about the licence

- Performing Right Society Ltd, for musical performances. The Centre for Education and Finance Management administers this licence
- Phonographic Performance Ltd, for playing recorded music. The Centre for Education and Finance Management administers this licence
- The Mechanical Copyright Protection Society, for making CDs and DVDs containing copyright music. The Centre for Education and Finance Management administers this licence
- Filmbankmedia and Motion Picture Licensing Company for showing films
- Christian Copyright Licensing International for copying and projecting hymns and other Christian music

If you require a copy of any of these licences, or further information about them, you should contact the relevant copyright management organisation (or, where applicable, its agent) listed above.

The DfE encourages schools to make the best use of these licences. For example, the Educational Recording Agency offers links to broadcast resources and provides a collection of case studies showing how teachers use television and radio effectively in their lessons.

The Mechanical Copyright Protection Society licence allows schools to make recordings of student performances and sell copies to generate income.

The licences don't cover:

- images on websites, unless the website is covered by the CLA or NLA Media Access – you can check using CLA's Check Permissions tool
- content accessed directly from YouTube
- some extra-curricular activities, for example showing films to a paying audience; please contact the relevant organisation

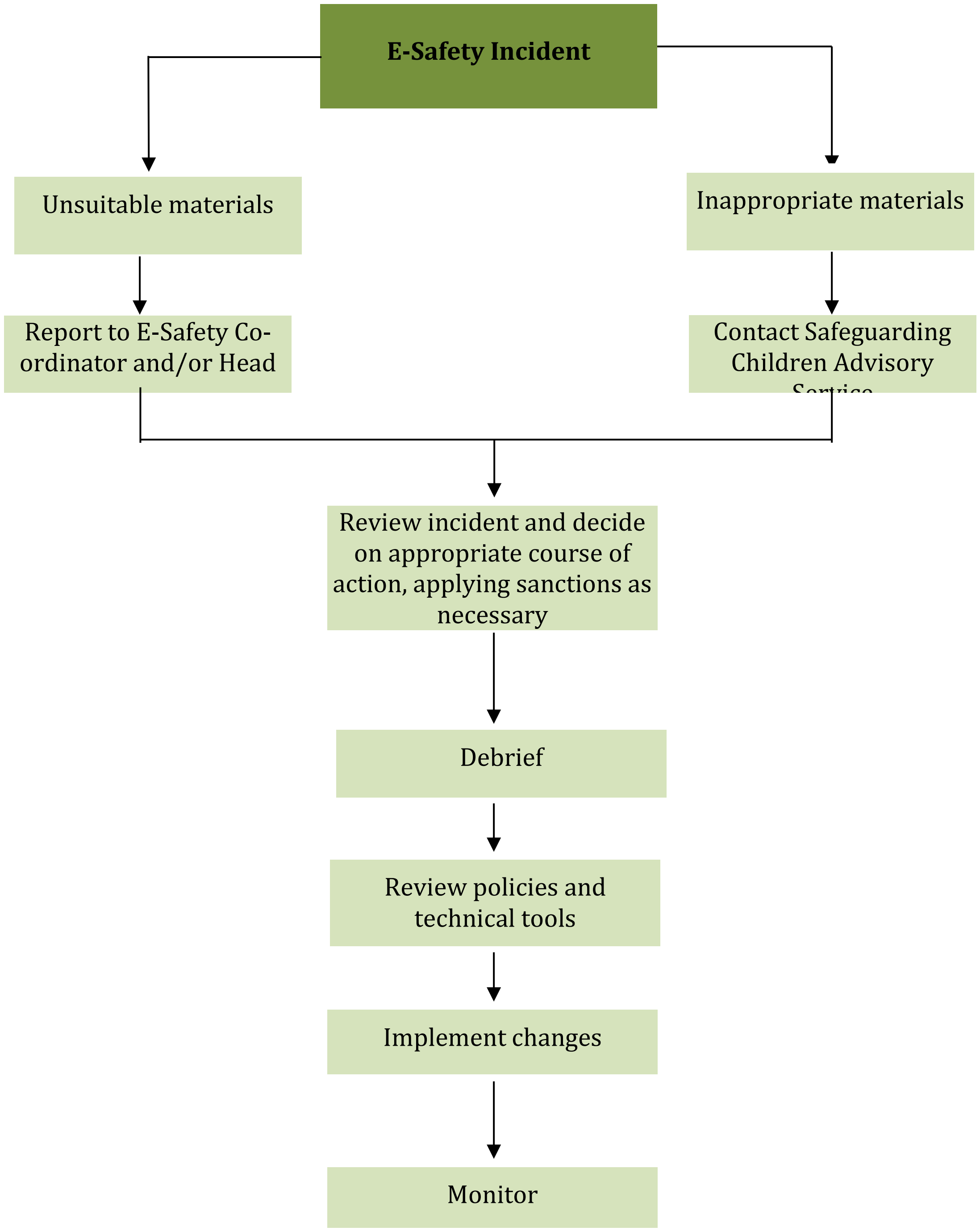
The CLA's Check Permissions tool enables you to check whether you can copy from a particular publication under the terms of the CLA and NLA Media Access licences. (Remember that images copied under these licences are covered for internal distribution within the school, but not for sharing on a public facing website.) It also helps you to check whether you can copy from a particular publication under the terms of the Schools Printed Music Licence.

APPENDIX A: E-SAFETY AUDIT – TO BE UNDERTAKEN BY ALL SCHOOLS

This quick self-audit will help the senior management team assess whether the e-safety basics are in place.

Does the school/Trust have an e-safety policy that complies with CYPD guidance?	
Date of latest update:	
The Policy was agreed by Trustees on:	
The Policy is available for staff at:	
The policy is available for pupils at:	
The designated Child Protection Officer is:	
The e-safety co-ordinator is:	
Has e-safety training been provided for both pupils and staff?	
Is the Think U Know training being considered?	
Do all staff sign an ICT Code of Conduct on appointment?	
Do parents sign and return an agreement that their child will comply with the School's e-safety rules?	
Have school e-safety rules been set for pupils?	
Are these rules displayed in all rooms with computers?	
Internet access is provided by an approved educational internet service provider and complies with DCSF requirements for safe and secure access.	
Has the school filtering policy been approved by the senior management team?	
Is personal data collected, stored and used according to the principles of the Data Protection Act?	

APPENDIX B: FLOWCHART FOR RESPONDING TO E-SAFETY INCIDENTS IN SCHOOLS


E-Safety Incident
Unsuitable materials
Inappropriate materials
Report to E-Safety Co-ordinator and/or Head
Contact Safeguarding Children Advisory Service
Review incident and decide on appropriate course of action, applying sanctions as necessary
Debrief
Review policies and technical tools
Implement changes
Monitor

APPENDIX C: ONLINE SAFETY RESOURCES

National Agencies

Child Exploitation and Online Protection Centre (CEOP) homepage. Report concerns to CEOP via the "Make a Report" button: https://www.ceop.police.uk/safety-centre/

Think U Know website. Advice for parent, teachers and young people. Includes teaching resources. : https://www.thinkuknow.co.uk/

Internet Watch Foundation. Report illegal content online.: https://www.iwf.org.uk/

Childnet International – Guidance for parents, teachers, children and young people. https://www.childnet.com/

UK Safer Internet Centre - https://www.saferinternet.org.uk/

NEN E-Safety (The Education Network) - https://www.nen.gov.uk/

E-Safety Curriculum Materials

ThinkUKnow – Material from CEOP aimed at children aged 4 to 16 (KS1 to KS4) https://www.thinkuknow.co.uk/

Welcome to the Web (KS2/3) - http://www.w2tw.uk/

Ideas to inspire Internet safety (KS1/2) - https://www.saferinternet.org.uk/advice-centre/young-people/resources-3-11s

Guidance for schools - https://www.gov.uk/government/organisations/uk-council-for-internet-safety

Internet Matters, contains guides and resources for both parents and teachers - https://www.internetmatters.org/

For Parents

Internet Matters, contains guides and resources for both parents and teachers - https://www.internetmatters.org/

Think U Know website. Advice for parent, teachers and young people. https://www.thinkuknow.co.uk/

Online security advice from the BBC - http://www.bbc.co.uk/webwise/topics/safety-and-privacy/