Transform Trust

Online/E-Safety Policy

June 2020

Introduction

Information Communication and Technology (ICT) in the 21st Century is seen as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, schools need to build in the use of these technologies in order to arm our children with the skills to access lifelong learning and employment.

ICT covers a wide range of resources including: web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of ICT within our society as a whole.

The impact of Covid-19 in 2020 has seen a dramatic increase in the use of virtual platforms such as MSTeams and Zoom to support regular communication with both staff and children.

Currently, the Internet technologies children and young people are using both inside and outside of the classroom include:

- Websites
- Learning platforms and virtual learning environments
- Email and instant messaging
- Chat rooms and social networking
- Blogs and wikis
- Podcasting
- Video broadcasting
- Music downloading
- Gaming
- Mobile/smart phones/tv's with text, video and/or web functionality
- Other mobile devices with web functionality

Whilst exciting and beneficial both in and out of the context of education, much ICT, particularly web-based resources are not consistently policed. All users need to be aware of the range of risks associated with the use of these Internet technologies.

At Transform Trust we understand the use of technology has become a significant component of many safeguarding issues. Child sexual exploitation; radicalisation; sexual predation and technology often provides the platform that facilitates harm. We expect our schools to have an effective approach to online safety that will empower them to protect and educate children in their use of technology and to establish mechanisms to identify, intervene in, and escalate any incident where appropriate.

The breadth of issues classified within online safety is considerable but can be categorised into three areas of risk:

a. **Content** – being exposed to illegal, inappropriate or harmful material; for example pornography, fake news, racist or radical and extremist views;

b. **Contact** – being subjected to harmful online interaction with other users; for example commercial advertising as well as adults posing as children or young adults; and
c. **Conduct** – personal online behaviour that increase the likelihood of, or causes, harm; for example making, sending and receiving explicit images, or online bullying *(KCSIE, Sept 2020)*.

Our schools will teach children the appropriate behaviours and critical thinking to enable them to remain both safe and legal when using the Internet and related technologies in and beyond the context of the classroom.

This Policy is inclusive of both fixed and mobile Internet; technologies provided by the school such as PCs, laptops, iPads, smart TVs, digital video equipment and technologies owned by pupils and staff, but brought onto school premises such as laptops, mobile camera phones, portable media players and smart watches.

Scope of the Policy

This Policy applies to all members of the *(insert school name)* (including staff, pupils, volunteers, parents/carers, visitors and other adults) who have access to and are users of the school's digital technology systems, both in and out of school.

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of online-bullying or other online safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data.

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate online safety behaviour that take place out of school.

Roles and Responsibilities

As online safety is an important aspect of strategic leadership within the schools, the Headteachers and Transform Trust Board ultimately have responsibility to ensure that this policy and practices are embedded and monitored. Schools should have a named Online/E-Safety Lead who may also have other responsibilities across the school. All members of the school communities should be made aware of who their Online/E-Safety Lead is. It is the role of the Online/E-Safety Lead to keep abreast of current issues and guidance through organisations such CEOP (child exploitation and online protection), Childnet, ThinkuKnow, NSPCC (see Appendix 4 for further information and support websites).

The Headteacher and/or Online/E-Safety Lead should update Senior Leaders and Governors to ensure that all Senior Leaders and Governors have an understanding of the issues at their school in relation to local and national guidelines and advice.

The following section outlines the online safety roles and responsibilities of individuals and groups within the school.

a. Transform Trust Board

Trustees have delegated this Policy to the Guardians Group and they are responsible for the approval of the Online/E-Safety Policy and for reviewing the effectiveness of the policy. Trustees and Local Governing Bodies through their named Safeguarding Governors will be required to undergo regular safeguarding training and the requirement to ensure children are taught about safeguarding, including online and that online safety training for staff is integrated, aligned and considered as part of the overarching safeguarding approach.

b. Headteachers and Senior Leaders

- The Headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day to day responsibility for online safety will be delegated to the Online/E-Safety Lead.
- The Headteacher and (at least) another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff. See flowchart (Appendix 1) on dealing with online safety incidents.
- The Headteacher and Senior Leaders are responsible for ensuring that the Online/E-Safety Lead and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.
- The Headteacher and Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out monitoring of online safety.
- The Senior Leadership Team will receive termly monitoring reports from the Online/E-Safety Lead.

c. Online/E-Safety Lead

- Takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies/documents.
- Ensures that the school's website is accurate and appropriate in terms of online learning and e-safety.
- Ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- Provides training and advice for staff.
- Contributes to the wider development of online safety across the Trust.
- Support the development of the online/e-safety curriculum.
- Liaises with the Digital Lead in school to ensure that virtual learning is safe and secure.
- Liaises with school technical staff.
- Assess emerging technologies for educational benefit and a risk assessment will be carried out by the school before it is used.
- Ensure that any new technology has a Data Protection Impact Assessment (DPIA) prior to installation; and that where appropriate an Information Sharing Agreement is in place by

liaising with the School's Data Controller (Headteacher) and/or the Trust's Data Protection Officer.

- Ensure there are online/e-safety posters displayed in and around school and on the school's website.
- Receives reports of online safety incidents and creates a log of incidents to inform future online safety developments.
- Meets regularly with Senior Leaders to discuss current issues, review incident logs and filtering/change control logs.
- Reports regularly to Senior Leadership Team.

d. Technical Staff

Those with technical responsibilities are responsible for ensuring:

- That the school's technical infrastructure is secure and is not open to misuse or malicious attack.
- That the school meets required online safety technical requirements and any other Trust guidance that may apply.
- That users may only access the networks and devices through a properly enforced password protection system.
- That they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant.
- That the use of the networks/internet/digital technologies is regularly monitored in order that any misuse/attempted misuse can be reported to the Headteacher and Senior Leaders; Online/E-Safety Lead and/or Lead DSL for investigation.
- That monitoring software/systems are implemented and updated as agreed in school policies.

e. Teaching, Support Staff and other Adults

Are responsible for ensuring that:

- they have an up to date awareness of online safety matters and of the current school's Online/E-Safety policy and practices
- they have read, understood and signed the staff acceptable use agreement (see Appendix 2)
- they adhere to the procedures when using virtual platforms such as Zoom/MSTeams
- they report any suspected misuse or problem to the Headteacher/Senior Leader/Online/E-Safety Lead or Lead DSL for investigation/action/sanction
- all digital communications with pupils/parents/carers should be on a professional level and only carried out using official school systems
- online safety issues are embedded in all aspects of the curriculum and other activities
- pupils understand and follow the Online/E-Safety Policy and acceptable use agreements (see Appendix 2)
- pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor the use of digital technologies, mobile devices, cameras, etc. in lessons and other school activities (where allowed) and implement current policies with regard to these devices

- in lessons where internet use is pre-planned pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

f. Designated Safeguarding Lead

Should be trained in online safety issues and be aware of the potential for serious child protection/safeguarding issues to arise from:

- sharing of personal data
- access to illegal/inappropriate materials
- inappropriate on-line contact with adults/strangers
- potential or actual incidents of grooming
- online-bullying

g. Pupils

- Pupils are responsible for using the school's digital technology systems in accordance with the pupil acceptable use agreement (see Appendix 2).
- Pupils will have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- Pupils need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- Pupils will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking/use of images and on online-bullying.
- Pupils should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's Online/E-Safety policy covers their actions out of school, if related to their membership of the school.

h. Parents/carers

Parents/carers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website, social media and information about national/local online safety campaigns/literature. Parents and carers will be encouraged to support the school in promoting good online safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- access to parents' sections of the website/learning platform
- parents who are responsible for using the school's digital technology systems in accordance with the parent acceptable use agreement (see Appendix 2).
- *their children's personal devices in the school (where this is allowed)*

i. Community Users

External organisations using any of our school's ICT facilities must adhere to our Online/E-Safety Policy. It is up to the school to ensure that a copy of this Policy is provided and/or available.

Policy Statements

Education – Pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in online safety/digital literacy is therefore an essential part of the school's online safety provision. Children need the help and support of the school to recognise and avoid online safety risks and build their resilience.

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned online safety curriculum should be provided as part of computing/PHSE/other lessons and should be regularly revisited.
- Key online safety messages should be reinforced as part of a planned programme of assemblies and pastoral activities.
- Pupils should be taught in all lessons, including lessons delivered remotely through the school's virtual platform, to be critically aware of the materials/content they access on-line and be guided to validate the accuracy of information (see Appendix 3 for remote learning guidance).
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- Pupils should be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making. *(Note: additional duties for schools under the Counter Terrorism and Securities Act 2015 which requires schools to ensure that children are safe from terrorist and extremist material on the internet)*.
- Pupils should be helped to understand the need for the pupil acceptable use agreements (see Appendix 2) and encouraged to adopt safe and responsible use both within and outside school.
- Staff should act as good role models in their use of digital technologies, the internet and mobile devices.
- In lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Pupils will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils.
- It is illegal for children under the age of 13 to have social media accounts. However, we accept that some pupils will still use them, school will advise them never to give out personal details of any kind, which may identify them or their location.
- Pupils are advised to set and maintain profiles on such sites to maximum privacy and deny access to unknown individuals.
- Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.
- It is accepted that from time to time, for good educational reasons, pupils may need to research topics (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff can temporarily remove those

sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

Education – Parents/Carers

Many parents and carers have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring/regulation of the children's online behaviours. Parents may underestimate how often children come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

Parents/Carers will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils. However, we accept that some pupils will still use them, school will advise them never to give out personal details of any kind, which may identify them or their location.

The school will therefore seek to provide information and awareness to parents and carers through:

- *Curriculum activities*
- *Letters, newsletters, website, learning platform*
- *Parents/carers evenings/sessions*
- *High profile events/campaigns e.g. Safer Internet Day*
- *Reference to the relevant information and support websites (see Appendix 4)*

Education – The Wider Community

The school will provide opportunities for local community groups/members of the community to gain from the school's online safety knowledge and experience. This may be offered through the following:

- Providing *fam*ily learning courses in use of new digital technologies, digital literacy and online safety
- Online safety messages targeted towards grandparents and other relatives as well as parents.
- The school website will provide online safety information for the wider community.
- Sharing their online safety expertise/good practice with other local schools.
- Supporting community groups e.g. Early Years Settings, Childminders, youth and sports/voluntary groups to enhance their online safety provision.

Education and Training – Staff, Other Adults and Volunteers

It is essential that all staff receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A planned programme of formal online safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out regularly.
- All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the school's Online/E-Safety policy and acceptable use agreements.
- It is expected that some staff will identify online safety as a training need.
- The Online/E-Safety Lead will receive regular updates through attendance at training events and by reviewing guidance documents released by relevant organisations.

- This Online/E-Safety policy and its updates will be presented to and discussed by staff in staff/team meetings/training sessions.
- The Online/E-Safety Lead will provide advice/guidance/training to individuals as required.

Training – Governors and Trustees

Governors and Trustees should take part in online safety training/awareness sessions, with particular importance for those who are members of any group involved in technology/online safety/health and safety/safeguarding. This may be offered in a number of ways:

- Online through the commissioned training platform by the Trust (currently SSS Learning).
- Participation in school training/information sessions for staff or parents.

Technical – infrastructure/equipment, filtering and monitoring

The school will be responsible for ensuring that the school's infrastructure and network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their online safety responsibilities:

- School technical systems will be managed in ways that ensure that the school meets recommended technical requirements by the Trust.
- There will be regular reviews and audits of the safety and security of school's technical systems.
- Servers, wireless systems and cabling must be securely located and physical access restricted.
- All users will have clearly defined access rights to school technical systems and devices.
- All users (at KS2?) will be provided with a username and secure password by *(insert name or title)* who will keep an up to date record of users and their usernames. Users are responsible for the security of their username and password. (Schools may choose to use group or class logons and passwords for KS1 and below, but should consider whether this models good password practice and need to be aware of the associated risks)
- The "master/administrator" passwords for the school systems, used by the Network Manager (or other person) must also be available to the Headteacher or other nominated Senior Leader and kept in a secure place.
- *(Insert name or role)* is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations.
- Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored. There is a clear process in place to deal with requests for filtering changes.
- Internet filtering/monitoring should ensure that children are safe from terrorist and extremist material when accessing the internet.
- The school has provided enhanced/differentiated user-level filtering (allowing different filtering levels for different ages/stages and different groups of users – staff/pupils etc).
- School technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the acceptable use agreement.

- An appropriate system is in place for users to report any actual/potential technical incident/security breach to the relevant person, as agreed (Data Protection Incident Log held by schools).
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices, etc. from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual devices are protected by up to date virus software.
- An agreed procedure is in place for the provision of temporary access of "guests" (e.g. trainee teachers, supply teachers, visitors) onto the school systems.
- An agreed procedure is in place regarding the extent of personal use that users (staff/pupils/community users) and their family members are allowed on school devices that may be used out of school.
- An agreed procedure is in place that allows staff to/forbids staff from downloading executable files and installing programmes on school devices.
- An agreed procedure is in place regarding the use of removable media (e.g. memory sticks/CDs/DVDs) by users on school devices. Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

Mobile Technologies (including BYOD/BYOT)

Mobile technology devices may be school owned/provided or personally owned and might include: smartphone, tablet, notebook/laptop or other technology that usually has the capability of utilising the school's wireless network. The device then has access to the wider internet which may include the school's learning platform and other cloud based services such as email and data storage.

All users should understand that the primary purpose of the use mobile/personal devices in a school context is educational. The mobile technologies policy should be consistent with and inter-related to other relevant school polices including but not limited to the safeguarding policy, behaviour policy, bullying policy, acceptable use policy, and policies around theft or malicious damage. Teaching about the safe and appropriate use of mobile technologies should be an integral part of the school's online safety education programme.

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents/carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for online-bullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.

- Written permission from parents or carers will be obtained before photographs or videos of pupils are published on the school website/social media/local press. Parents/Carers may withdraw their permission at any time.
- In accordance with guidance from the Information Commissioner's Office, parents/carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published/made publicly available on social networking sites, nor should parents/carers comment on any activities involving other pupils in the digital/video images.
- Staff and volunteers are allowed to take digital/video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment; the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital/video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission.
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Pupil's work can only be published with the permission of the pupil and parents or carers.

Data Protection

With effect from 25th May 2018, the data protection arrangements for the UK changed following the European Union General Data Protection Regulation (GDPR). As a result, schools are likely to be subject to greater scrutiny in their care and use of personal data. More detailed guidance is available in our Data Protection Policy. Personal data will be recorded, processed, transferred and made available according to the current data protection legislation.

IT security is ensured and regularly checked. Patches and other security essential updates are applied promptly to protect the personal data on the systems. Administrative systems are securely ring-fenced from systems accessible in the classroom/to learners.

Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. When using communication technologies, the school considers the following as good practice:

- The official school email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored. Staff and pupils should therefore use only the school email service to communicate with others when in school, or on school systems (e.g. by remote access).
- Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any communication that makes them feel uncomfortable, is offensive,

discriminatory, threatening or bullying in nature and must not respond to any such communication.

- Any digital communication between staff and pupils or parents/carers (email, social media, class dojo (or similar systems) chat, blogs, etc) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or social media must not be used for these communications.
- Whole class/group email addresses may be used at KS1, while pupils at KS2 and above will be provided with individual school email addresses for educational use.
- Pupils should be taught about online safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

Social Media - Protecting Professional Identity

All school have a duty of care to provide a safe learning environment for pupils and staff. Schools could be held responsible, indirectly for acts of their employees in the course of their employment.

Staff members who harass, engage in online bullying, discriminate on the grounds of sex, race or disability or who defame a third party may render the school or Transform Trust liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

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

- Ensuring that personal information is not published.
- Training is provided including: acceptable use; social media risks; checking of settings; data protection; reporting issues.
- Clear reporting guidance, including responsibilities, procedures and sanctions.
- Risk assessment, including legal risk.

School staff should ensure that:

- No reference should be made in social media to pupils, parents/carers or school staff without explicit consent.
- They do not engage in online discussion on personal matters relating to members of the school community.
- Personal opinions should not be attributed to the school or Transform Trust.
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

When official school social media accounts are established there should be:

- A process for approval by Senior Leaders.
- Clear processes for the administration and monitoring of these accounts – involving at least two members of staff.
- A code of behaviour for users of the accounts, including:

- Systems for reporting and dealing with abuse and misuse
- Understanding of how incidents may be dealt with under school disciplinary procedures.

Personal Use:

- Personal communications are those made via a personal social media accounts. In all cases, where a personal account is used which associates itself with the school or impacts on the school or Transform Trust, it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy.
- Personal communications which do not refer to or impact upon the school are outside the scope of this policy.
- Where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken.
- The school permits reasonable and appropriate access to private social media sites.

Monitoring of Public Social Media:

- As part of active social media engagement, it is considered good practice to pro-actively monitor the Internet for public postings about the school.
- The school should effectively respond to social media comments made by others according to a defined policy or process.
- The school's use of social media for professional purposes will be checked regularly by Senior Leaders and the Online/E-Safety Lead to ensure compliance with the school policies.

Assessing Risks

All schools will take reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school, nor the Trust, can accept liability for the material accessed, or any consequences of internet access. The school will audit IT provision to establish if the online/e-safety procedures are adequate and that its implementation is effective.

Dealing with unsuitable/inappropriate activities

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned from school and all other technical systems. Other activities e.g. cyber-bullying would be banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would be inappropriate in a school context, either because of the age of the users or the nature of those activities.

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

User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	Child sexual abuse images – the making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978					X
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					X
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) contrary to the Criminal Justice and Immigration Act 2008					X
	Criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986					X
	Pornography				X	
	Promotion of any kind of discrimination				X	
	Threatening behaviour, including promotion of physical violence or mental harm				X	
	Promotion of extremism or terrorism				X	
	Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				X	
Activities that might be classed as cyber-crime under the Computer Misuse Act: • Gaining unauthorised access to school networks, data and files, through the use of computers/devices • Creating or propagating computer viruses or other harmful files • Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords) • Disable/Impair/Disrupt network functionality through the use of computers/devices • Using penetration testing equipment (without relevant permission) Offences may result in the Police being notified.						X

Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school or Trust.				X	
Revealing or publicising confidential or proprietary information (e.g. financial/ personal information, databases, computer/network access codes and passwords)				X	
Unfair usage (downloading/uploading large files that hinders others in their use of the internet)				X	
Using school systems to run a private business				X	
Infringing copyright				X	
Online gaming (educational)					
Online gaming (non-educational)				X	
Online gambling				X	
Online shopping/commerce		X			
File sharing		X			
Use of social media	X				
Use of messaging apps	X				
Use of video broadcasting e.g. Youtube		X			

Responding to incidents of misuse

This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident.

Illegal Incidents

If there is any suspicion that the website(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right hand side of the flowchart (see Appendix 1) for responding to online safety incidents and report immediately to the police.

Other Incidents

It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow school policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse. In the event of suspicion, all steps in this procedure should be followed:

- Have more than one senior member of staff involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by adult/child and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.

- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below).
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does, then appropriate action will be required and could include the following:
    - Internal response or discipline procedures.
    - Involvement of the Executive Team of the Trust.
    - Police involvement and/or action.
- If content being reviewed includes images of child abuse, then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:
    - Incidents of 'grooming' behaviour.
    - The sending of obscene materials to a child.
    - Adult material which potentially breaches the Obscene Publications Act.
    - Criminally racist material.
    - Promotion of terrorism or extremism.
    - Offences under the Computer Misuse Act (see User Actions chart above).
    - Other criminal conduct, activity or materials.
- Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.

It is important that all of the above steps are taken as they will provide an evidence trail for the school, Trust and possibly the police and demonstrate that visits to these sites were carried out for safeguarding purposes. The completed form should be retained by the group for evidence and reference purposes.

School Actions and Sanctions

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with in line with school and Trust policies.

Staff and the Online/E-Safety Policy

- All staff will be given a copy of this policy and its importance explained.
- Staff should be aware that internet traffic could be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Any ICT device issued to staff remains the property of the school. Users of such equipment should therefore adhere to this policy.

Handling Online/E-Safety Complaints

- Complaints of Internet misuse will be dealt with by a Senior Leader in school and reported to the Online/E-Safety Lead.
- Complaints of a child protection nature must be dealt with in accordance with the school's child protection procedures.
- All schools must publish their Complaints policy online.

Writing and Reviewing the Online/E-Safety Policy

This policy includes a number of Acceptable Use Agreements for:

- Staff (which can be adopted for governors, visitors and contractors);
- parents/guardians
- pupils – split KS1 and KS2

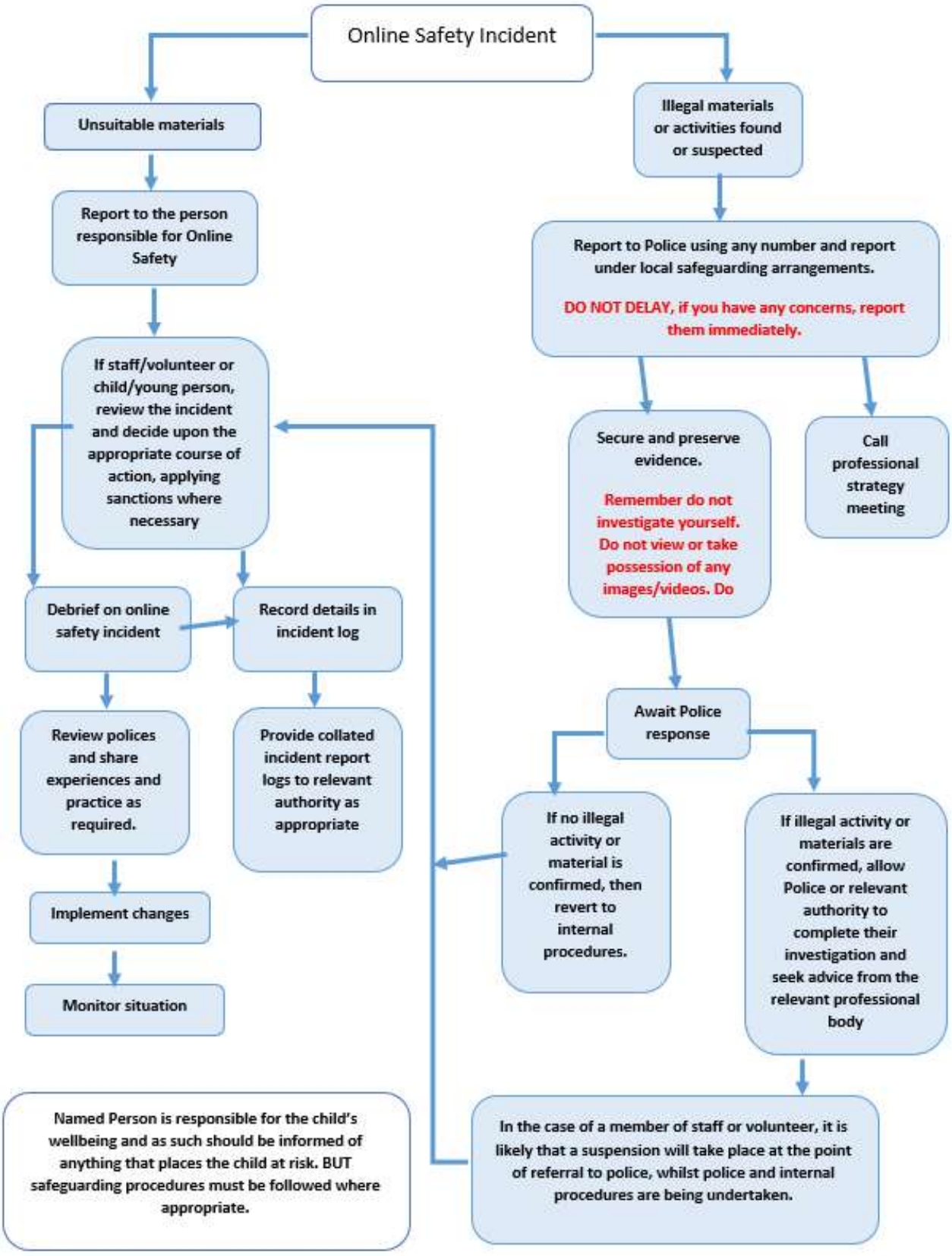
these are to protect the interests and safety of the whole school community. They are linked to other mandatory and school safeguarding policies such as safeguarding and child protection, behaviour, health & safety and anti-bullying etc.

Our Online/E-Safety Policy has been approved by the Trust's Guardians (Transform Trust's Safeguarding Group). The Online/E-Safety Policy will be reviewed bi-annually.

Monitoring and Review

This policy is implemented by schools on a day-to-day basis by all school staff and is monitored by the Online/E-Safety Lead.

Appendix 1: Flowchart – Illegal Incidents



Appendix 2: Acceptable Use Agreements

Acceptable Use Agreement: Trust/School Staff

This agreement covers use of all digital technologies while in Transform/School, at home or an external venue: i.e. email, internet, intranet, network resources, learning platform, software, communication tools, social networking tools, school website, apps and other relevant digital systems provided by Transform/School.

This agreement also covers Transform/School equipment when used inside or outside of Transform/School, use of online systems provided by Transform/School when accessed from inside or outside Transform/School, and posts on social media made from outside Transform/School premises/hours which reference the Trust/School (and communities thereof), or which might bring Transform/School or your professional status into disrepute.

It also covers use of personal or 3rd party devices used to access Transform/School or Transform/School related digital technologies, which could include mobile phones, tablets, laptops, PCs, smart watches or any other non-Transform/School provided device.

School regularly reviews and updates their Acceptable Use Agreements to ensure that they are consistent and up to date with digital advances.

We expect all employees to act professionally and with integrity at all times, ensuring that appropriate safeguards are taken when using Transform/School equipment, accessing Transform/School systems and interacting with others both internally and externally. For avoidance of doubt, this includes all personal and Transform/School issued mobile devices. This agreement is designed to keep everyone safe and to be fair to others.

Please note that Trust/School systems and users are protected and monitored by security and filtering services to provide safe access to digital technologies. Your behaviour online when representing Trust/School on all Trust/School/Personal devices whether in Trust/School or otherwise may therefore be subject to monitoring.

- I understand that I have a responsibility for my own and others' e-safeguarding and I undertake to be a 'safe and responsible digital technologies user'; and that I am responsible for all content, including browser history on my Trust/School (and Personal when Trust/School related) device.
- I understand that it is my responsibility to ensure that I remain up-to-date and understand the Trust/School's most recent online safety/safeguarding policies, including Keeping Children Safe in Education.
- I will report any accidental access to, or receipt of inappropriate materials, or filtering breach or equipment failure to the Trust's Chief Finance Officer.

- I will not download any software or resources from the internet that can compromise the Trust network or might allow me to bypass the filtering and security system or are not adequately licensed.
- I understand that it is my responsibility to take appropriate security measures for the safe keeping of my device and report any damage, loss or theft immediately to the Trust's Chief Finance Officer. Please check that you have appropriate insurance cover in the event of loss or theft of any Trust device from your car for example.
- I will only connect any device (including Trust issued encrypted USB flash drive), to the network that has up-to-date anti-virus software, and I will keep any 'loaned' equipment up-to-date, using the Trust's recommended anti-virus and other ICT 'defence' systems.
- I am aware that under the provisions of the GDPR (General Data Protection Regulation), the Trust has extended responsibilities regarding the creation, use, storage and deletion of data, and I will not store any pupil data that is not in line with the Trust/school's data policy and adequately protected. The Trust data protection officer must be aware of all data storage.
- I understand that all statutory responsibilities relating to the job role should be upheld at all times when handling/using data.
- I understand that failure to comply with this agreement could lead to my device being removed and if necessary further investigation undertaken.

User Signature

I agree to abide by all the points above.

Signature: …… Date: ……

Print Name: ……

Job Title: ……

Key Stage 1: Acceptable Use Agreement

This is how I keep **SAFE online**:	✓
1. I only use the devices I'm **ALLOWED** to	
2. I **CHECK** before I use new sites, games or apps	
3. I **ASK** for help if I'm stuck	
4. I **THINK** before I click	
5. I **KNOW** people online aren't always who they say	
6. I don't keep ~~**SECRETS**~~ just because someone asks me to	
7. I don't change **CLOTHES** in front of a camera	
8. I am **RESPONSIBLE** so never share private information	
9. I am **KIND** and polite to everyone	
10. I **TELL** a trusted adult if I'm worried, scared or just not sure	

My trusted adults are: _____ at school

_____ at home and _____

My name is _____

KS2 Pupil Online Acceptable Use Agreement

This agreement will help keep me safe and help me to be fair to others

- ***I am an online digital learner*** – I use the school's internet and devices for schoolwork, homework and other activities to learn and have fun. I only use sites, games and apps that my trusted adults say I can.
- ***I am a secure online learner*** – I keep my passwords to myself and reset them if anyone finds them out.
- ***I am careful online*** – I think before I click on links and only download when I know it is safe or has been agreed by trusted adults. I understand that some people might not be who they say they are, so I should be very careful when someone wants to be my friend.
- ***I am private online*** – I only give out private information if a trusted adult says it's okay. This might be my home address, phone number or other personal information that could be used to identify me or my family and friends.
- ***I keep my body to myself online*** – I never change what I wear in front of a camera and remember that my body is mine and mine only, and I don't send any photos without checking with a trusted adult.
- ***I say no online if I need to*** – if I get asked something that makes me worried or upset or just confused, I say no, stop chatting and tell a trusted adult.
- ***I am a rule-follower online*** – I know that some websites and social networks have age restrictions and I respect this; I only visit sites, gams and apps that my trusted adults have agreed to.
- ***I am considerate online*** – I do not join in with bullying or sharing inappropriate material.
- ***I am respectful online*** – I do not post, make or share unkind, hurtful or rude messages/comments and tell my trusted adults if I see these.
- ***I am part of a community*** – I do not make fun of anyone or exclude them because they are different to me. If I see anyone doing this, I tell a trusted adult.
- ***I am responsible online*** – I keep others safe by talking to my trusted adults if a friend or person I know is being bullied or harassed or is worried or upset by things they read, watch or hear.
- ***I don't do public live streams on my own*** – and only go on a video chat if my trusted adult knows I am doing it and who with.

- ***I communicate and collaborate online*** – with people I know and have met in real life or that a trusted adult knows about.
- ***I am SMART online*** – I understand that unless I have met people in real life, I can't be sure who someone is online, so if I want to meet someone for the first time, I must always ask a trusted adult for advice.
- ***I am a creative digital learner online*** – I don't just spend time online to look at things from other people; I get creative to learn and make things! I only edit or delete my own digital work and only use other people's with their permission or where it is copyright free or has a Creative Commons licence.
- ***I am a researcher online*** – I use safer search tools approved by my trusted adults. I understand that not everything online can be believed, but I know how to check things and know to 'double check' information I find online.

I have read and understood this agreement. I know who are my trusted adults are and agree to the above.

Pupil Name: …… Date: ……..

Parent/Carer Acceptable Use Agreement

<<School name>> regularly reviews and updates all Acceptable Use documents to ensure that they are consistent with the school Online/E-Safety and Safeguarding Policies, <<which can be found at…>>. We attempt to ensure that all pupils have good access to digital technologies to support their teaching and learning and we expect all our students to agree to be responsible users to help keep everyone safe and to be fair to others.

Your child will be asked to read and sign an Acceptable Use Agreement tailored to his/her age. Please read this carefully – it is <<attached to this form for reference // available online at XXXXX>>.

Parent/Carer Acceptable Use Agreement

Internet and IT: As the parent or legal guardian of the pupil(s) named below, I grant permission for the school to give my *daughter/son* access to:

- the internet at school
- the school's chosen email system
- <<name any online 'managed learning environment', Google Classroom, Microsoft for Education tools, or similar>>
- IT facilities and equipment at the school

I accept that ultimately the school cannot be held responsible for the nature and content of materials accessed through the internet and mobile technologies, but I understand that the school takes every reasonable precaution to keep pupils safe and to prevent pupils from accessing inappropriate materials.

I understand that all internet and device use in school is subject to filtering and monitoring; I understand that all school-owned devices used outside of school may also be subject to filtering and monitoring, and should be used in the same manner as when in school.

Use of digital images, photography and video: I understand the school has a clear policy on "The use of digital images and video" and I support this.

I understand that the school will necessarily use photographs of my child or including them in video material to support learning activities where I have given consent.

I accept that the school may use photographs/video that includes my child in publicity that reasonably promotes the work of the school (where I have given consent), and for no other purpose.

Social networking and media sites: I understand that the school has a clear policy on "The use of social networking and media sites" and I support this. The impact of social media use is often felt in schools, and this is why we expect certain behaviours from pupils when using social media at all times.

I will not take and then share online, photographs, videos etc., about other children (or staff) at school events, without permission.

I understand that the school takes any inappropriate behaviour seriously and will respond to observed or reported inappropriate or unsafe behaviour.

I understand that my son/daughter has agreed in the pupil acceptable-use policy not to search for or share any material that could be considered offensive, harmful or illegal. This might include bullying or extremist/hate/discriminatory content.

I will support the school by promoting safe and responsible use of the internet, online services and digital technology at home. I will inform the school if I have any concerns.

Name of child: ……..

Name of parent/guardian: ……

Signature of parent/guardian: ……

Date: ……

The use of digital images and video

To comply with the General Data Protection Regulation (GDPR) (which supersedes the 1998 Data Protection Act), we need your permission before we can photograph or make recordings of your daughter/son.

<<School name>> rules for any external use of digital images are:

If the pupil is named, we avoid using their photograph.
If their photograph is used, we avoid naming the pupil.

Where showcasing examples of pupils' work we only use their first names, rather than their full names. If showcasing digital video work to an external audience, we take care to ensure that pupils aren't referred to by name on the video, and that pupils' full names aren't given in credits at the end of the film.

Only images of pupils in suitable dress are used.

Staff are not allowed to take photographs or videos on their personal equipment.

Examples of how digital photography and video may be used at school include:

- Your child being photographed (by the class teacher or teaching assistant) as part of a learning activity, e.g. taking photos or a video of progress made by a nursery child, as part of the learning record and then sharing with their parent/guardian.
- Your child's image being used for presentation purposes around the school, e.g. in class or wider school wall displays or PowerPoint© presentations.
- Your child's image being used in a presentation about the school and its work in order to share its good practice and celebrate its achievements, which is shown to other parents, schools or educators, e.g. in our school prospectus or on our school website. On rare occasions, your child's picture could appear in the media if a newspaper photographer or television film crew attends an event.

  Note: If we, or you, actually wanted your child's image linked to their name we would contact you separately for permission, e.g. if they won a national competition and wanted to be named in local or government literature.

The use of social networking and online media

This school asks its whole community to promote the 'three commons' approach to online behaviour:

- **Common courtesy**
- **Common decency**
- **Common sense**

How do we show common courtesy online?

- We ask someone's permission before uploading photographs, videos or any other information about them online.
- We do not write or upload 'off-hand', hurtful, rude or derogatory comments and materials. To do so is disrespectful and may upset, distress, bully or harass.

How do we show common decency online?

- We do not post comments that can be considered as being intimidating, racist, sexist, homophobic or defamatory, or encourage extremist views. This is online bullying and may be harassment or libel.
- When such comments exist online, we do not forward such emails, tweets, videos, etc. Creating or forwarding such materials can make us liable for prosecution.

How do we show common sense online?

- We think before we click.
- We think before we upload comments, photographs and videos.
- We think before we download or forward any materials.
- We think carefully about what information we share with others online, and we check where it is saved and check our privacy settings.
- We make sure we understand changes in use of any websites we use.
- We block harassing communications and report any abuse.

Any actions online that impact on the school and can potentially lower the school's (or someone in the school) reputation in some way or are deemed as being inappropriate will be responded to.

If any member of staff, student or parent/carer is found to be posting libellous or inflammatory comments on the internet or any social media, they will be reported to the appropriate 'report abuse' section of the network site (all social media have clear rules about content which can be posted and have robust mechanisms to report breaches). Pupils and staff would be disciplined appropriately, and we expect parents to support us in this and behave appropriately themselves.

In serious cases, we will also consider legal options to deal with any such misuse.

The whole school community is reminded of the CEOP process for reporting inappropriate sexual approaches towards children at thinkuknow.co.uk/parents.

Appendix 3 Remote Learning Guidance

	Teachers	Pupils	Parents
Only use school registered accounts	✓	✓	
Sit against a neutral background in a safe and neutral space	✓	✓	
Do not use a system that has not been approved by the school	✓		
Consider those children without internet access	✓		
Ensure all settings are as they should be e.g. chat and recording	✓		
Be aware of rules and guidelines for chat and communication	✓	✓	
Consider any specific needs for vulnerable, including Looked After Children and those with Special Educational Needs and Disabilities	✓		
Ensure two adults are present for video calls or class learning	✓		
Avoid one to one sessions unless pre-approved	✓		
Don't share personal information	✓	✓	
Be mindful of background noise	✓		✓
Abide by acceptable use agreements	✓	✓	✓
Be aware of reporting procedures – staying safe online or safeguarding concerns	✓	✓	✓
Consider whether you want to record and inform all participants if you are	✓		
Be aware of procedure for asking for help if stuck	✓	✓	
Gain/Give consent	✓		✓
Ensure knowledge of system and how to use safely	✓	✓	✓

Appendix 4 Information and Support

The following list is not exhaustive but should provide a useful starting point:

Advice for Transform Trust, Governors and Senior Leaders

- Childnet provide guidance for schools on cyberbullying
- Educateagainsthate provides practical advice and support on protecting children from extremism and radicalisation
- London Grid for Learning provides advice on all aspects of a school or college's online safety arrangements
- NSPCC provides advice on all aspects of a school or college's online safety arrangements
- Safer recruitment consortium "guidance for safe working practice", which may help ensure staff behaviour policies are robust and effective
- Searching screening and confiscation is departmental advice for schools on searching children and confiscating items such as mobile phones
- South West Grid for Learning provides advice on all aspects of a school or college's online safety arrangements
- Use of social media for online radicalisation - A briefing note for schools on how social media is used to encourage travel to Syria and Iraq
- UK Council for Internet Safety have provided advice on sexting-in-schools-and- colleges and using-external-visitors-to-support-online-safety-education

Remote education, virtual lessons and live streaming

- Case studies on remote education practice are available for schools to learn from each other
- Departmental guidance on safeguarding and remote education including planning remote education strategies and teaching remotely
- London Grid for Learning guidance, including platform specific advice
- National cyber security centre guidance on choosing, configuring and deploying video conferencing
- National cyber security centre guidance on how to set up and use video conferencing
- UK Safer Internet Centre guidance on safe remote learning

Support for children

- Childline for free and confidential advice
- UK Safer Internet Centre to report and remove harmful online content
- CEOP for advice on making a report about online abuse

Parental support

- Childnet offers a toolkit to support parents and carers of children of any age to start discussions about their online life, to set boundaries around online behaviour and technology use, and to find out where to get more help and support
- Commonsensemedia provide independent reviews, age ratings, & other information about all types of media for children and their parents
- Government advice about protecting children from specific online harms such as child sexual abuse, sexting, and cyberbullying
- Government advice about security and privacy settings, blocking unsuitable content, and parental controls
- Internet Matters provide age-specific online safety checklists, guides on how to set parental controls on a range of devices, and a host of practical tips to help children get the most out of their digital world
- Let's Talk About It provides advice for parents and carers to keep children safe from online radicalisation
- London Grid for Learning provides support for parents and carers to keep their children safe online, including tips to keep primary aged children safe online
- Lucy Faithfull Foundation StopItNow resource can be used by parents and carers who are concerned about someone's behaviour, including children who may be displaying concerning sexual behaviour (not just about online)
- National Crime Agency/CEOP Thinkuknow provides support for parents and carers to keep their children safe online
- Net-aware provides support for parents and carers from the NSPCC and O2, including a guide to social networks, apps and games
- Parentzone provides help for parents and carers on how to keep their children safe online
- Parent info from Parentzone and the National Crime Agency provides support and guidance for parents from leading experts and organisations
- UK Safer Internet Centre provide tips, advice, guides and other resources to help keep children safe online