Online Safety Policy

TEACH
The Educational Alliance of Canford Heath

RIGHTS RESPECTING SCHOOL
UNICEF

Statement of Intent

Our mission is to promote a love of learning in order to maximise the life chances of every child in our Trust. Through nurturing, high expectations and skilled teaching, we will have a lasting and positive impact on our local and wider community.

Our Vision

The TEACH Trust supports our children to become empowered citizens that make a meaningful contribution to society. Our curriculum reflects our locality and all it offers and aims to educate all children in matters which affect humanity in the wider world: these include all matters that relate to the climate and the world around us, such as climate change; the importance of respecting and celebrating the importance of equality and diversity; and being responsible global citizens.

We have the highest aspirations for our children: the broad and balanced curriculum promotes learning, provides cultural capital and supports spiritual, moral, social and cultural development. The Rights Respecting Gold awards and Anti Bullying awards reflect some of many ways in which education for character are integral to the work of our schools and highlights our focus on the children's personal development.

We aim to inspire our children to be socially conscious individuals who make a difference to the world. All our children secure the key learning and skills they will need to become lifelong learners and gain employment. Our ultimate aim is to improve all our children's life chances and prepare them to thrive in their future lives.

Under the Equality Act 2010 and the Public Sector Equality Act which came into force in April 2011, the Trust has due regard to the need to eliminate discrimination, advance equality of opportunity and foster good relations.

Scope of the Policy

This policy applies to all members of the academy community (including staff, students / pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of academy ICT systems, both in and out of the academy.

The Education and Inspections Act 2006 empowers Headteachers to such an extent as is reasonable, to regulate the behaviour of pupils when they are off the academy site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying or other Online Safety incidents covered by this policy, which may take place outside

of the academy, but is linked to membership of the academy. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

The academy 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

The following section outlines the online safety roles and responsibilities of individuals and groups within the academy:

CEO and Headteacher:

- The CEO and 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 DSL.
- The CEO and Headteacher are aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff.
- The Headteacher is responsible for ensuring that the E Safety Leads 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 CEO and Headteacher will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.

School E-Safety Leads:

- takes responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies / documents
- 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
- liaises with the Local Authority / relevant body
- liaises with school technical staff
- receives reports of online safety incidents and creates a log of incidents to inform future online safety developments, *It is my understanding that this report goes to HT and DHT only.*

- attends relevant meetings
- reports regularly to Senior Leadership Team

IT Manager:

The IT Manager and technical staff are responsible for ensuring:

- that the TEACH Trust technical infrastructure is secure and is not open to misuse or malicious attack
- that TEACH Trust meets required online safety technical requirements and any Local Authority Online Safety Policy / Guidance that may apply.
- that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed

Teaching and Support Staff

Are responsible for ensuring that:

- they have an up to date awareness of online safety matters and of the current academy Online Safety Policy and practices
- they have read, understood and signed the Staff Acceptable Use Policy (AUP) and the IT Code of Practice for Use of Computers by Staff
- they report any suspected misuse or problem to the IT manager and Headteacher for investigation / action / sanction
- all digital communications with students / pupils / parent(s) / carer(s) should be on a professional level and only carried out using official school systems

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
- cyber-bullying

Pupils:

- are responsible for using TEACH trust digital technology systems in accordance with the Pupil Acceptable Use Agreement

Parent(s) / Carer(s)

Parent(s) / Carer(s) play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. TEACH Trust will take every opportunity to help parent(s)/carer(s) understand these issues through parents' evenings, newsletters, letters, website and information about national / local online safety campaigns / literature. Parent(s) and carer(s) will be encouraged to support the Trust 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 parent/carer sections of the website and on-line student / pupil records
- their children's personal devices in the academy (where this is allowed)

Community Users

When applicable Community Users who access academy systems / website as part of the wider TEACH trust provision will be expected to sign a Community User AUA before being provided with access to academy systems.

Policy Statements

Education – Students / 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 is therefore an essential part of TEACH Trust online safety provision. Children and young people 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 to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.
- 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. Nb. additional duties for schools / academies 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 Agreement and encouraged to adopt safe and responsible use both within and outside TEACH Trust..
- 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.

Education – Parent(s) / Carer(s)

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 on-line behaviours. Parent(s)/carer(s) may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The academy will therefore seek to provide information and awareness to parent(s) and carer(s) through:

- Curriculum activities
- Letters, newsletters, web site,
- Parent / Carer evenings / sessions
- High profile events / campaigns e.g. Safer Internet Day
- Reference to the relevant web sites / publications e.g. swgfl.org.uk www.saferinternet.org.uk/ http://www.childnet.com/parents-and-carers

Education & Training – Staff / 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 academy Online Safety Policy and Acceptable Use Agreements.

It is expected that some staff will identify online safety as a training need within the performance management process.

- The E-Safety Leads will receive regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisations.
- This Online Safety Policy and its updates will be presented to and discussed by staff in staff / team meetings / INSET days.
- The E-Safety Leads will provide advice / guidance / training to individuals as required

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.

Remote Learning

Remote Learning occurs when the learner and instructor, or source of information, are separated by time and distance and therefore cannot meet in a traditional classroom setting. During times that Remote Learning is essential, an online classroom will be used to continue lessons using pre-recorded videos and copies of the tasks.

It is essential that all staff, parent(s)/carer(s) and children know and understand their roles and responsibilities when using the online classroom/remote learning.

Staff

- Have an understanding of how to use the online classroom to set work for children working remotely.
- Will monitor the children's attendance using the online classroom.
- Will record any 'live contact' with children for safeguarding of all participants, including phone calls.

- Will ensure tasks are accessible via online classroom and the work is in line with the needs of the children and curriculum.
- Will be dressed appropriately and working from a suitable room during live contact with parent(s)/carer(s) and children.
- Will offer support and feedback to children to ensure progress for all learners.
- Will report any concerns to the school's Designated Safeguarding Lead/Deputy Head teacher.

Parent(s)/carer(s) and children

- Understand that all online activity can carry risk if misused and I will supervise my child to ensure they use digital technologies safely.
- Will supervise my child's use of the online classroom, ensuring that they use it as directed by the teacher.
- Understand that the school will monitor my child's activity when using the login provided by the school.
- Understand that any live contact between school staff and children will be recorded by the school for the safeguarding of all participants.
- Will ensure that my child does not make any form of recording or screen capture of teachers or other users.
- Will ensure that my child is dressed appropriately and working from a suitable room (ideally not a bedroom) during any live contact with teachers.
- Are aware that other children might see or hear me and my child and anything in the background during any live contact
- Understand that if I have any concerns regarding online safety, these should be reported to the school's Designated Safeguarding Lead/Deputy Headteacher.

Technical – infrastructure / equipment, filtering and monitoring

TEACH Trust will be responsible for ensuring that the 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:

- Academy technical systems will be managed in ways that ensure that TEACH Trust meets recommended technical requirements
- There will be regular reviews and audits of the safety and security of academy technical systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to academy technical systems and devices.
- All users will be provided with an initial username and secure password by the IT Manager. Passwords have to be renewed by staff users every 90 days. The school's systems enforce the change and required complexity requirements. Passwords can be changed by the IT Manager at any time to allow account access and to block users accessing accounts and systems.

- Users are responsible for the security of their username and password
- The “master / administrator” passwords for the school / academy ICT system, used by the IT Manager (or other persons) must also be available to the CEO/Headteacher or other nominated senior leader and kept in a secure place (eg school / academy safe)
- The IT manager 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 (Inadequate licencing could cause the school to breach the Copyright Act which could result in fines or unexpected licensing costs)
- 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 should ensure that children are safe from terrorist and extremist material when accessing the internet.
- The academy has provided differentiated user-levels
- 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 workstations are protected by up to date virus software.
- An agreed policy is in place for the provision of temporary access of “guests” (eg trainee teachers, supply teachers, visitors) onto the school systems.

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 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 TEACH BYOD Policy, 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.

TEACH Trust allows	School Devices			Personal Devices		
	School owned for single user	**School owned for multiple users**	**Authorised device[1]**	**Student owned**	**Staff owned**	**Visitor owned**
Allowed in school	*Yes*	*Yes*	*Yes*	*No*	*Yes*	*Yes*
Full network access	*Yes*	*Yes*	*Yes*	*No*	*No*	*No*
Internet only				*No*	*YES*	*Yes*

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, parent(s) / carer(s) and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying 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 parent(s) or carer(s) will be obtained before photographs of students / pupils are published on the school website / social media / local press
- In accordance with guidance from the Information Commissioner's Office, parent(s) / carer(s) are welcome to take videos and digital images of their children at school / academy 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 parent(s) / carer(s) 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 academy policies concerning the sharing, distribution and publication

of those images. Those images should only be taken on academy equipment, and 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 academy 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 student / pupil and parent(s) or carer(s).

Data Protection

Personal data will be recorded under General Data Protection Regulations 2017 (GDPR), processed, transferred and made available. GDPR states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure

The school / academy must ensure that:

- It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.
- Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.
- All personal data will be fairly obtained in accordance with the "Privacy Notice" and lawfully processed in accordance with the "Conditions for Processing".
- It has a Data Protection and Confidentiality Policy
- It is registered as a Data Controller for the purposes of the GDPR Act.
- Responsible persons are appointed / identified - Data Manager and Data Controller
- Risk assessments are carried out
- It has clear and understood arrangements for the security, storage and transfer of personal data
- Data subjects have rights of access and there are clear procedures for this to be obtained

- There are clear and understood systems for the deletion and disposal of data
- There is a policy for reporting, logging, managing and recovering from information risk incidents
- There are clear Data Protection clauses in all contracts where personal data may be passed to third parties
- There are clear policies about the use of cloud storage / cloud computing which ensure that such data transfer / storage meets the requirements laid down by the Information Commissioner's Office.

Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
- Transfer data using encryption and secure password protected devices.

When personal data is stored on any portable computer system, memory stick or any other removable media:

- the data must be encrypted and password protected
- the device must be password protected
- the device must offer approved virus and malware checking software
- the data must be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete

COMMUNICATIONS

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the school currently considers the benefit of using these technologies for education outweighs their risks / disadvantages:

Communication Technologies	Staff & other adults				Students / Pupils			
	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to the school / academy**					Yr 6		Yr 5/6	
Use of mobile phones in lessons								
Use of mobile phones in social time								
Taking photos on mobile cameras								
Use of other mobile devices e.g. tablets, gaming devices								
Use of personal email addresses in school / academy , or on school / academy network								
Use of school / academy email for personal emails***								
Use of messaging apps								
Use of social media								
Use of blogs								

** Staff and other adults – stored in staff areas, not on their person

Students/pupils – stored in the school office, not on their person

*** Personal use of the teachpoole domain is under certain conditions

When using communication technologies the school / academy considers the following as good practice:

- The official *school / academy* email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored.
- Users must immediately report, to the nominated person – in accordance with the 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 students / pupils or parent(s) / carer(s) (email, social media, chat, blogs, VLE etc) must be professional in tone and content.

- Students / 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 TEACH Trust website and only official email addresses should be used to identify members of staff.

Social Media - Protecting Professional Identity

All schools, academies and local authorities have a duty of care to provide a safe learning environment for pupils and staff. Schools/academies and local authorities could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, cyberbully, discriminate on the grounds of sex, race or disability or who defame a third party may render TEACH Trust liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

TEACH Trust 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

TEACH Trust staff should ensure that:

- No reference should be made in social media to students / pupils including ex-pupils, parent(s) / carer(s) or school TEACH Trust staff
- 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 TEACH trust
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information

When official TEACH Trust 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,
- Systems for reporting and dealing with abuse and misuse

- Understanding of how incidents may be dealt with under school / academy 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 TEACH Trust, or impacts on TEACH Trust, it must be made clear that the member of staff is not communicating on behalf of the Trust 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
- TEACH Trust 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

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 / academy 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.

TEACH Trust believes that the activities referred to in the following section would be inappropriate in a context and that users, as defined below, should not engage in these activities in / or outside the TEACH Trust schools when using school / academy equipment or systems. The school / academy policy restricts usage as follows:	Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal

User Actions

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	
Using school systems to run a private business					X	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school / academy					X	
Infringing copyright					X	
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)					X	
Creating or propagating computer viruses or other harmful files					X	
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)					X	

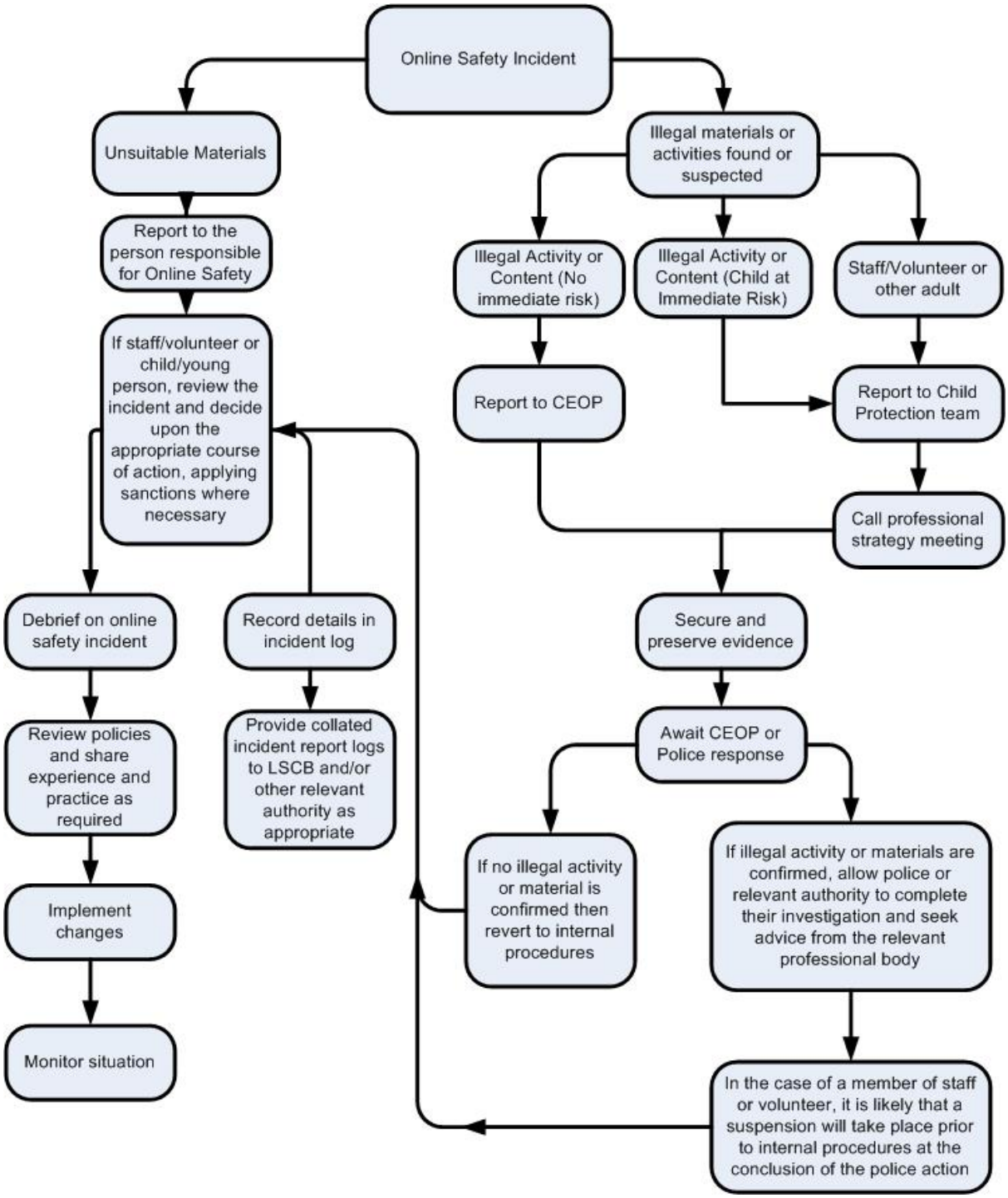
On-line gaming (educational)	x				
On-line gaming (non-educational)				x	
On-line gambling				x	
On-line shopping / commerce	x				
File sharing				x	
Use of social media		x			
Use of messaging apps		x			
Use of video broadcasting e.g. Youtube		x			

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. Incidents might involve illegal or inappropriate activities (see “User Actions” above).

Illegal Incidents

If there is any suspicion that the web site(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 (below) for responding to online safety incidents and report immediately to the police.



Other Incidents

It is hoped that all members of the school / academy community will be responsible users of digital technologies, who understand and follow school / academy 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 / volunteer 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 young people 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 by Local Authority / Academy Group or national / local organisation (as relevant).
    - 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
    - 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 TEACH 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.

Actions & Sanctions

It is more likely that the academy 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. It is intended that incidents of misuse will be dealt with through normal behaviour / disciplinary procedures as follows:

	Actions / Sanctions								
Students / Pupils Incidents	Refer to class teacher	Refer to Year Leader	Refer to HT/CEO	Refer to Police	Refer to technical support staff for action re filtering / security etc.	Inform parent(s)/ carer(s)	Removal of network / internet access rights	Warning	Further sanction eg detention / exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		X	X	X					
Unauthorised use of non-educational sites during lessons	X								
Unauthorised / inappropriate use of mobile phone / digital camera / other mobile device		X							
Unauthorised / inappropriate use of social media / messaging apps / personal email		x							

Unauthorised downloading or uploading of files		X							
Allowing others to access school / academy network by sharing username and passwords		x							
Attempting to access or accessing the school / academy network, using another student's / pupil's account		x							
Attempting to access or accessing the school / academy network, using the account of a member of staff			x						
Corrupting or destroying the data of other users			x						
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature			x			x			
Continued infringements of the above, following previous warnings or sanctions			x			x	x	x	
Actions which could bring the school / academy into disrepute or breach the integrity of the ethos of the school			x			x		x	
Using proxy sites or other means to subvert the school's / academy's filtering system			x					x	
Accidentally accessing offensive or pornographic material and failing to report the incident		x				x		xx	
Deliberately accessing or trying to access offensive or pornographic material			x			x			x
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act		x						x	

Staff Incidents	Refer to line manager	Refer to HT/CEO	Refer to Local Authority	Refer to Police	Refer to Technical Support Staff for action re filtering etc.	Warning	Suspension/investigation	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		X	X	X			x	x
Inappropriate personal use of the internet / social media / personal email		x				x	x	

Unauthorised downloading or uploading of files	x							
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account		x				x		
Careless use of personal data e.g. holding or transferring data in an insecure manner		x				x		
Deliberate actions to breach data protection or network security rules		x						x
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		x						x
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature		x					x	x
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils		x					x	x
Actions which could compromise the staff member's professional standing		x					x	x
Actions which could bring the school / academy into disrepute or breach the integrity of the ethos of the school / academy		x					x	x
Using proxy sites or other means to subvert the school's / academy's filtering system		x					x	x
Accidentally accessing offensive or pornographic material and failing to report the incident		x				x		
Deliberately accessing or trying to access offensive or pornographic material		x	x	x			x	x
Breaching copyright or licensing regulations		x				x		
Continued infringements of the above, following previous warnings or sanctions		x	x	x			x	x

Reviewed March 2021

Reviewed December 2022

Reviewed January 2024

Online Safety Policy

Equality Impact Assessment

Question	Response	
Which relevant groups and stakeholders have been consulted with in relation to this policy?		Please tick
	Pupils	
	Trustees	✓
	Staff	✓
	Parents/Carers	
	Local Authority	
	Trade Unions	
	Other Advisors (give details)	~~LA – Safeguarding audit~~
What are the arrangements for monitoring and reviewing the actual impact of the policy?	Termly	
	Annually	✓
	When applied	
	If legislation changes	✓
	If a formal complaint	✓

Does the policy affect one group less or more favourably than another on the basis of:	**Y/N**
Disability	N
Gender reassignment	N
Marriage or civil partnership	N
Pregnancy and maternity	N
Race	N
Religion or belief	N
Sexual orientation	N
Sex (gender)	N
Age	N
SEN	N
Vulnerable	N
Traveller, migrant, refugees and people seeking asylum	N
EAL	N

	Y/N	**Comments/Actions**
Is there any evidence that some groups are affected differently?	N	
If you have identified potential discrimination, are any exceptions valid, legal and/or justifiable?	n/a	
Is the impact of the policy likely to be negative?	N	
If yes, can the impact be mitigated by taking different action?	n/a	