ONLINE SAFETY POLICY

Scope of the policy

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

t+centres provides a safe environment for pupils to lean and does all that is reasonably possible to limit children's exposure to on line abuse through school IT systems. t+centres ensure that appropriate filtering and monitoring systems are in place, which are regularly reviewed for their effectiveness. t+centres ensure that the SMT and relevant staff are aware and understand the provisions in place and manage them effectively and know how to escalate identified concerns. SMT will identify those at potentially greater risk of harm and how often they access the IT systems.

t+centres provides a safe environment for pupils to learn and does all that is reasonably possible

The Education and Inspections Act 2006 empowers Principals to such extent as is reasonable, to regulate the behaviour of students 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 cyber-bullying, or other online incidents covered by this policy, which may take place outside of the school, but are 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. In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

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 behaviour that take place out of school.

The use of technology has become a significant component of many safeguarding issues. Child sexual exploitation; radicalisation; sexual predation; technology often provides the platform that facilitates harm. An effective approach to online safety empowers t+centres to protect and educate the whole school community in their use of technology and establishes mechanisms to identify, intervene in, and escalate any incident where appropriate.

t+centres recognises that, although the breadth of issues within online safety is considerable, it can be categorised into three areas of risk:

- **Content:** being exposed to illegal, inappropriate or harmful material such as pornography,

fake news, racist or radical and extremist views

- **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
- **Conduct:** Personal online behaviour that increases the likelihood of, or causes, harm; for example making, sending and receiving explicit images, or online bullying.

Roles and responsibilities

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

Governors

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about online incidents and monitoring reports. A member of the Governing Body has taken on the role of Online Safety Officer. The role of the Online Safety Governor will include:

- Regular meetings with the Online Safety Officer;
- Regular monitoring of online incident logs.

Principal and Senior Leadership Team

- The Principal has a duty of care for ensuring the safety (including online) of members of the school community, though the day-to-day responsibility for online safety will be delegated to the Online Safety Officer.
- The Director (Barry Coppins) 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 flow chart on dealing with online safety incidents, 'Responding to incidents of misuse' and relevant Local authority disciplinary procedures.
- The Director is responsible for ensuring that the Online Safety Officer 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 Director will ensure 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.
- The Senior Leadership Team will receive regular monitoring reports from the Online Safety Officer.

Online Safety Officer

- 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 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;
- Liaises with school technical staff;
- Receives reports of online safety incidents and creates a log of incidents to inform future online safety developments;
- Meets regularly with Online Safety Governor to discuss current issues, review incident logs and filtering / change control logs;
- Attends relevant meeting of Governors;
- Reports regularly to Senior Leadership Team.

Network technical provider

Will ensure that:

- 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 Local Authority 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;
- The filtering policy (if it has one), is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person;
- That they keep up to date with online 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 network / internet / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Online Safety Officer for investigation.

Teaching and Support Staff

Are responsible for ensuring that:

- They have an up to date awareness of online safety matters and of the current school online safety policy and practices;
- They have read, understood and signed the Staff Acceptable Use Agreement (AUP);
- They report any suspected misuse or problem to the Online Safety Officer for investigation;
- All digital communications with students / 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;
- Students understand and follow the online safety and acceptable use policies;
- Students 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 students 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.

Designated Safeguarding Lead and Deputy DSLs

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

Staff training and student awareness

Staff will be given training to help them understand the issues of radicalisation, to recognise the signs of vulnerability or radicalisation and know how to refer their concerns. This information also forms part of induction safeguarding training. Staff are updated as necessary in weekly briefings.

All staff were WRAP trained (Workshop to Raise Awareness of Prevent) in December 2015 and training is undertaken at regular intervals.

Prevent training .

Radicalisation and extremism awareness assembly and separate policy.

Any concerns should be referred to the designated Safeguarding Lead or Deputy DSLs.

Students / pupils

- Are responsible for using the school digital technology systems in accordance with the Student Acceptable Use Policy;
- Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations;
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so;
- 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 and the use of images and on cyber-bullying;
- Should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's Online Safety Policy covers their actions out of school, if related to their membership of the school.

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 newsletters, website and information about national and

local online safety campaigns.

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;
- their children's personal devices in the school (where this is allowed).

Policy Statements

Education – students

Whilst regulation and technical solutions are very important, their use must be balanced by educating students to take a responsible approach. The education of students in online safety is therefore an essential part of the school's 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 lessons and should be regularly revisited;
- Key online safety messages should be reinforced as part of a planned programme of assemblies;
- Students should be taught in all lessons to be critically aware of the materials and content they access online and be guided to validate the accuracy of information;
- Students should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet;
- Students should be helped to understand the need for the student Acceptable Use Agreement 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;
- Students are not allowed to freely search the internet; staff should be vigilant in monitoring the content of the websites the young people visit.

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 and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

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

- curriculum activities;
- letters, newsletters, website.

Education and 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 school online safety policy and Acceptable Use Agreements.
- The Online Safety Officer receives regular updates through attendance at external training events, CEOP, Think You Know, and other relevant organisations 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 meetings /and INSET days.
- The Online Safety Officer (or other nominated person) will provide advice, guidance and training to individuals as required.

Training – governors / directors

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

- Attendance at training provided by the Local Authority or other relevant organisation;
- Participation in school training and information sessions for staff or parents.

Technical – infrastructure / equipment, filtering and monitoring

The school will be responsible for ensuring that the school infrastructure 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.
- There will be regular reviews and audits of the safety and security of school 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 school technical systems and devices.
- All users will be provided with a username and secure password as required. Users are responsible for the security of their username and password.
- Marie Riddle 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.

- An appropriate system is in place, an online safety incident form, for users to report any actual or potential technical incident or security breach to the relevant person, as agreed.
- 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 byup to date virus software.
- An agreed policy is in place that allows staff to / forbids staff from downloading executable files and installing programmes on school devices.
- An agreed policy 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.

Bring Your Own Device (BYOD)

The educational opportunities offered by mobile technologies are being expanded as a wide range of devices, software and online services become available for teaching and learning, within and beyond the classroom. This has led to the exploration by schools of users bringing their own technologies in order to provide a greater freedom of choice and usability. However, there are a number of online safety considerations for BYOD that need to be reviewed prior to implementing such a policy. Use of BYOD should not introduce vulnerabilities into existing secure environments. Considerations will need to include; levels of secure access, filtering, data protection, storage and transfer of data, mobile device management systems, training, support, acceptable use, auditing and monitoring. This list is not exhaustive and a BYOD policy should be in place and reference made within all relevant policies.

- The school has a set of clear expectations and responsibilities for all users;
- The school adheres to the Data Protection Act principles;
- All users are provided with and accept the Acceptable Use Agreement;
- All network systems are secure and access for users is differentiated;
- Where possible these devices will be covered by the school's normal filtering systems, while being used on the premises;
- All users will use their username and password and keep this safe;
- Mandatory training is undertaken for all staff;
- Students / Pupils receive training and guidance on the use of personal devices;
- Regular audits and monitoring of usage will take place to ensure compliance;
- Any device loss, theft, change of ownership of the device will be reported as in the BYOD policy;
- Any user leaving the school will follow the process outlined within the BYOD policy.

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing

staff and students instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents/carers and students 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 students 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.
- 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 students / 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 students are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Students must not take, use, share, publish or distribute images of others without their permission.
- Photographs published on the website, or elsewhere, that include students will be selected carefully and will comply with good practice guidance on the use of such images.
- Students' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of students are published on the school website

Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which 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
- Only transferred to others with adequate protection.

t+centres will be GDPR compliant.

The school 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 Policy.
- It is registered as a Data Controller for the purposes of the Data Protection Act (DPA).
- Responsible persons are appointed.
- 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 policies and routines 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.

t+centres will be GDPR compliant.

Staff must ensure 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 with permission from the safeguarding officer.

- 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 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:

Zooms/online learning. (lockdown)

Throughout lockdown and on occasions there will be times when staff will be asked to Zoom call the students.

Where possible Zoom calls are to be made in school on school premises. To protect the staff, zoom calls can be recorded but must be shown to the head of centre of safeguarding lead at the end of each session.

The student has to be up and dressed ready for their lesson if a student is still in bed or lying in bed staff are asked to finish the call and let SLT know immediately so they can contact the students' parents.

ALL ZOOM CALLS MUST BE PASSWORD PROTECTED AND THE LINKS AND PASSWORDS TO BE SENT OUT TO THE PARENTS/ CARERS ONLY.

	Staff & other adults			Students				
Communication Technologies	Not 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 school		X		X				
Use of mobile phones in lessons	X			X				
Use of mobile phones in social time	X			X				
Taking photos on mobile phones / cameras	X			X				
Use of other mobile devices eg tablets, gaming devices	X					X		
Use of personal email addresses in school, or on school network	X			X				
Use of school email for personal emails	X			X				
Use of messaging apps	X			X				
Use of social media	X			X				
Use of blogs	X			X				

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.
- Users must immediately report, to the Designated Safeguarding Lead or a Deputy DSL, 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 students or parents / carers (email, chat, etc.) must be professional in tone and content.

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 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 the school or local authority liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

t+centres provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school through limiting access to personal information:

- Training to include: 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 students, parents / carers or school 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 school or local authority.
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

Unsuitable / inappropriate activities

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

User Actions		Acceptable	Acceptable at certain	Acceptable for nominated	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or	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 rounds of sexual orientation) - contrary to the Public Order Act 1986					X
comments that contain or relate to:	pornography				X	
	promotion of any kind of discrimination				X	
	threatening behaviour, including promotion of physical violence or mental harm				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 (e.g. 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	
Online gaming (educational)				X		

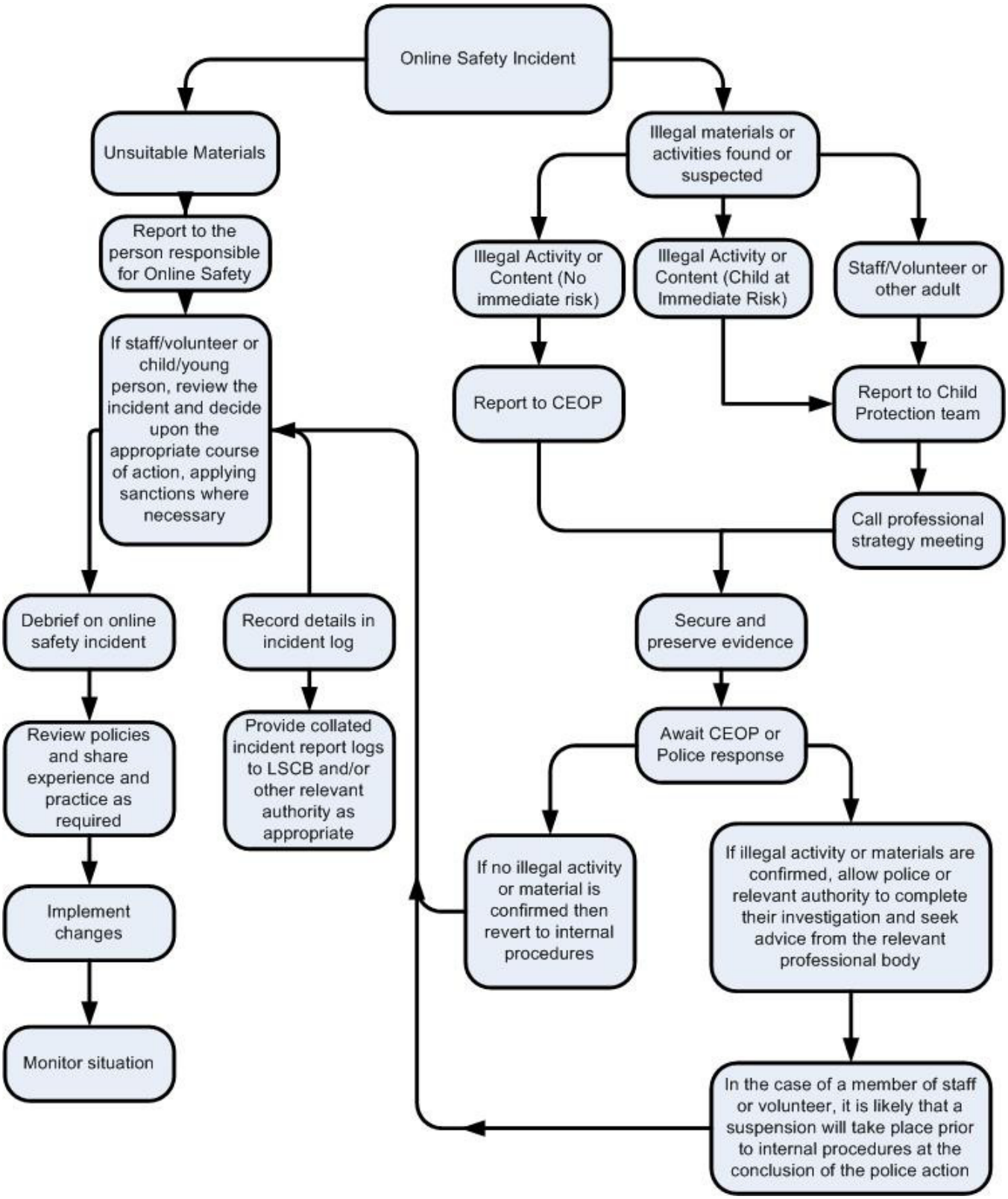
Online gaming (non educational)				X	
Online gambling				X	
Online shopping / commerce				X	
File sharing				X	
Use of social media				X	
Use of messaging apps				X	
Use of video broadcasting e.g. Youtube			X		

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

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 for responding to online safety incidents and report immediately to the police.


Online Safety Incident
Unsuitable Materials
Report to the person responsible for Online Safety
If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary
Debrief on online safety incident
Review policies and share experience and practice as required
Implement changes
Monitor situation
Record details in incident log
Provide collated incident report logs to LSCB and/or other relevant authority as appropriate
Illegal materials or activities found or suspected
Illegal Activity or Content (No immediate risk)
Illegal Activity or Content (Child at Immediate Risk)
Staff/Volunteer or other adult
Report to CEOP
Report to Child Protection team
Call professional strategy meeting
Secure and preserve evidence
Await CEOP or Police response
If no illegal activity or material is confirmed then revert to internal procedures
If illegal activity or materials are confirmed, allow police or relevant authority to complete their investigation and seek advice from the relevant professional body
In the case of a member of staff or volunteer, it is likely that a suspension will take place prior to internal procedures at the conclusion of the police action

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 / 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 or national / local organisation;
    - 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;
    - 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 and possibly the police and demonstrate that visits to these sites were carried out for child protection 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. It is intended that incidents of misuse will be dealt with through normal disciplinary procedures as follows:

Students **Actions / Sanctions**

Incidents:	Refer to class teacher / tutor	Refer to Online Safety Officer	Refer to Principal	Refer to Police	Refer to technical support staff for action re filtering / security etc	Inform parents / carers	Removal of network / internet access rights	Warning	Further sanction eg 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	X	X				X	
Unauthorised use of mobile phone / digital camera / other mobile device		X	X			X			
Unauthorised use of social media / messaging apps / personal email		X	X		X	X			
Unauthorised downloading or uploading of files		X			X				
Allowing others to access school / academy network by sharing username and passwords		X			X				
Attempting to access or accessing the school / academy network, using another student's / pupil's account		X			X				
Attempting to access or accessing the school / academy network, using the account of a member of staff		X	X		X				
Corrupting or destroying the data of other users		X	X		X	X			
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature		X	X	X	X				
Continued infringements of the above, following previous warnings or sanctions									X
Actions which could bring the school 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		X	X			
Deliberately accessing or trying to access offensive or pornographic material		X	X		X	X			
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act		X							

Staff **Actions / Sanctions**

Incidents:	Refer to line manager	Refer to Principal	Refer to Local Authority	Refer to Police	Refer to Technical Support Staff for	Warning	Suspension	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				
Inappropriate personal use of the internet / social media / personal email		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						
Careless use of personal data eg holding or transferring data in an insecure manner		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			X
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature		X						X
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students		X				X		
Actions which could compromise the staff member's professional standing		X						
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		X						

Using proxy sites or other means to subvert the school'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			
Breaching copyright or licensing regulations		X						
Continued infringements of the above, following previous warnings or sanctions		X						

History and implementation of this Online Safety Policy:

Accepted by SLT in this format:	September 2017
Approved by t+centres Governors:	September 2020
Last revised:	September 2023
To be reviewed:	September 2024 Or sooner in the light of any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place.

SLT, all staff and governors have read, discussed and contributed to this policy.

The Head of Centre will be responsible for ensuring all staff are briefed on the regulations and practice outlined in this policy.

The implementation of this Online Safety Policy will be monitored by the Online Safety Officer.

Should serious online safety incidents take place, the Designated Safeguarding Lead or a Deputy DSL should be informed.

t+centres follows guidelines from the Department of Education Publication: Filtering and Monitoring Standards. www.gov.uk/guidance/meeting-digital-and-technology-standards

Monitoring of this policy

The school will monitor the impact of the policy using:

- Logs of reported incidents
- Monitoring logs of internet activity (including sites visited)
- Internal monitoring data for network activity
- Surveys / questionnaires of
  - students / pupils
  - parents / carers

- staff / volunteers