CCE Digital Safeguarding Policy

January 2022

Scope of the Policy

This policy applies to all members of the Celtic Cross Education community (including staff, students / pupils, volunteers, parents / carers, contractors, visitors and community users) who have access to, and are users of, CCE ICT systems, both in and out of Celtic Cross Education and/or its schools.

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

The trust will deal with incidents within this policy and the associated Code of Conduct & IT Acceptable Use Policy and school behaviour and anti-bullying policies. Where known, staff will inform parents / carers of incidents of inappropriate online safeguarding behaviour that take place out of school.

2. Roles and Responsibilities

The following section outlines the digital safeguarding roles and responsibilities of individuals and groups within the Trust:

2.1. Trust Digital Safeguarding Co-ordinator:

Digital Safeguarding Coordinator= Shaun Perfect
Andrew Manning= Senior Network Engineer

The Digital Safeguarding Coordinator forms part of the Trust IT Group and the Designated Safeguarding Network that has wide representation from the Trust community. Wider members of the Trust involved in IT will assist the Digital Safeguarding Coordinator at each school with:
•supporting the Digital Safeguarding Coordinator in their role, with particular emphasis on sharing good practice and regular review.
•provide direction to Trust policy in regards to digital safeguarding.
•will assist in mapping and reviewing the digital safeguarding curriculum provision – ensuring relevance, breadth and progression.
•monitoring network / internet / incident logs.
•will consult with stakeholders – including parents / carers and the students / pupils about the digital safeguarding provision.
•will monitor improvement actions identified through SEF, 157 return and governance overviews.

2.2. Board of Directors:

The Trust Board are responsible for the approval of the Digital Safeguarding Policy. The Trust's digital safeguarding team will review the effectiveness of the policy, annually. Each safeguarding School Monitoring Councillor will oversee digital safeguarding at local school level.

2.3. Heads of School:

- The Head of School, also the named DSL, has a duty of care for ensuring the safety (including digital safeguarding) of members of the school community, though the day to day responsibility for digital safeguarding will be delegated to the Digital Safeguarding Co-ordinator.

- The Head of School and (at least) another member of the Senior Leadership Team / Senior Management Team should be aware of the procedures to be followed in the event of a serious digital safeguarding allegation being made against a member of staff (see flow chart on dealing with Digital Safeguarding incidents, included in a later section – "Responding to incidents of misuse" and relevant Trust disciplinary procedures).

- The Head of School and Digital Safeguarding Coordinator is responsible for ensuring that staff receive suitable training to enable them to carry out their digital safeguarding roles and to train other colleagues, as relevant.

- Each School's DSL will meet regularly with the DSC to receive updates and any specific feedback on their school. This opportunity will be given regularly by mutual attendance at the Trust IT group and Safeguarding group.

2.4. Digital Safeguarding Co-ordinator:

CCE's Digital Safeguarding Coordinator will:

- take day to day responsibility for digital safeguarding issues
- ensure that all staff are aware of the procedures that need to be followed in the event of a digital safeguarding incident taking place.
- liaise with the Trust's digital safeguarding team to get information, review current provision and arrange training.
- liaise with the Trust's IT team.
- receive reports of digital safeguarding incidents and create a log of incidents to inform future digital safeguarding developments.

2.5. External IT services by TME:

TME are responsible for ensuring:

- that the trust's technical infrastructure is secure and is not open to misuse or malicious attack.
- that users may only access the networks and devices through properly enforced password protection procedures.
- that, as an organisation, they keep up to date with digital safeguarding information in order to effectively carry out their role and to inform and update others as relevant.
- that the use of the Trust IT systems is regularly monitored in order that any misuse / attempted misuse can be reported to the Head of School / Digital Safeguarding Coordinator for investigation / action / sanction.
- that monitoring software / systems are implemented and updated, as necessary.

2.6. Teaching and Support Staff

Are responsible for ensuring that:

- they have an up to date awareness of digital safeguarding matters and comply with the Digital Safeguarding Policy and its practices.
- they have read, understood and signed the Staff Acceptable Use Policy (AUP)

- they report any suspected misuse or problem to the Head of School / DSL or Digital Safeguarding Coordinator for investigation / action / sanction.
- all digital communications with students / pupils / parents / carers should be on a professional level and only carried out using official school systems.
- Digital Safeguarding issues are embedded in all aspects of the curriculum and other activities.
- students / pupils understand and follow the Digital Safeguarding and acceptable use policies; staff help to facilitate and embed this culture.
- students / 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 and implement current policies with regard to these devices.
- in lessons, where internet use is pre-planned, younger pupils should be guided to sites checked as suitable for their use; protocols are in place for dealing with any unsuitable material that is found in internet searches. Older pupils will be supported in using the internet independently.

2.7. Child Protection / Safeguarding Designated Person

Designated Safeguarding Leads should be trained in Digital Safeguarding 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

2.8. Students / pupils:

Should need:

- to have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- to be expected to know and understand policies and or procedures for use of mobile devices and digital cameras in school. They should also know and understand procedures on the taking / use of images, and on cyber-bullying.
- should understand the importance of adopting good digital safeguarding practice when using digital technologies out of school and realise that the Trust's Digital Safeguarding Policy covers their actions out of school, if related to their membership of the school.

2.9. 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. CCE will take every opportunity to help parents understand these issues through parents' evenings, relevant advertising in newsletters, letters, website / VLE and information about national / local digital safeguarding campaigns / literature. Parents and carers will be encouraged to support each school in promoting positive digital safeguarding 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 / VLE and on-line student / pupil records.

- their children's personal devices in school , where this is allowed.

3. Policy Statements

3.1. Education – students / pupils

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

Digital safeguarding should be a focus in all areas of the curriculum and staff should reinforce digital safeguarding messages throughout the curriculum. The digital safeguarding curriculum should be broad, relevant and provide progression, with opportunities for creative activities.

The curriculum will be provided in the following ways:

- A planned digital safeguarding curriculum should be provided as part of Computing & IT, PSHE & RSHE. Internet safety should be embedded across all curriculum subjects and should not just be taught as a stand-alone subject.
- Key digital safeguarding messages should be reinforced as part of a planned programme of collective worship / pastoral activities.
- Students / 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.
- Students / 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 encouraged to adopt safe and responsible use of digital devices, both within and outside of 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.
- Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.

3.2 Education – parents / carers

Many parents and carers have only a limited understanding of digital safeguarding 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. 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 and parent participation.
- The sharing of information via letters, newsletters, web site & VLEs.
- Parents / Carers evenings / sessions.
- High profile events- campaigns like Safer Internet Day, for example.
- Reference to relevant web sites / publications

3.3 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 online safety training will be made available to staff. This will be regularly updated and reinforced via the online FLICK learning platform. It is expected that some staff will identify digital safeguarding as a training need within the performance management process and will seek and complete relevant training.
- All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the school's Digital Safeguarding Policy and Acceptable Use Policy.
- The Digital Safeguarding Coordinator will receive regular updates through attendance at external training events (eg from SWGfL / LA / other relevant organisations) and by reviewing guidance documents released by relevant organisations.
- This Digital Safeguarding Policy, and its updates, will be presented to, and discussed, by staff who will sign the policy to demonstrate that they understand the content and will abide by the terms set out.
- The Digital Safeguarding Coordinator (or other nominated person) will provide advice / guidance / training to individuals, as required/requested.

4. Technical – infrastructure / equipment, filtering and monitoring

The Trust will be responsible for ensuring that its infrastructure / 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 digital safeguarding responsibilities:

- Trust IT systems will be managed in ways that ensure that the trust meets recommended technical requirements.
- There will be regular reviews and audits of the safety and security of trust/school technical systems including backup procedures.
- All users will have clearly defined access rights to trust technical systems and devices.
- All users at KS2 and above will be provided with a username and secure password by TME 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 log-ins and passwords for KS1 and below.
- Internet access is filtered for all users. Illegal content 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.
- The school has provided enhanced / differentiated user-level filtering.
- Trust technical staff regularly monitor and record the activity of users on the trust's technical systems and users are made aware of this in the Acceptable Use Policy.
- An appropriate system is in place for users to report any actual / potential technical incident / 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 trust/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 trust/school systems.

- The Staff Acceptable Usage Policy forbids staff from downloading executable files and installing programmes on school devices.
- An agreed policy is in place (Staff Acceptable Use Policy) regarding the use of removable media (eg 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.

5. Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students / 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 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, which are:

1) 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.
2) 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 is 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.
3) Staff are allowed to take digital / video images to support educational aims, but must follow school protocols 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.
4) Care should be taken when taking digital / video images that students / pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
5) Students / pupils must not take, use, share, publish or distribute images of others without their permission.
6) Photographs published on the website, or elsewhere that include pupils, will be selected carefully and will only feature pupils who have permission for their image to be shared.
7) Students' full names will not be used anywhere on a website or blog, particularly in association with photographs.
8) Written permission from parents or carers will be obtained before photographs of pupils are published on the school website.
9) Pupils' work can only be published with the permission of the pupil and parents or carers.

6. 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.

CCE 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".
- CCE has a Board approved Data Protection Policy
- CCE is registered as a Data Controller for the purposes of the Data Protection Act (DPA)
- Responsible persons are appointed / identified - Data Protection Officer (DPO, Glyn Pascoe dpo@ict4.co.uk)
- Risk assessments are carried out, as necessary.
- CCE 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.
- There are clear policies about the use of cloud storage / cloud computing which ensure that such data 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.
- Lock their screen, if leaving their workstation temporarily.
- Transfer data using encryption and secure password protected devices and use SharePoint as a means of sharing personal information within the organisation.
- Ensure that encrypted email is used when sending personal information out of the organisation.
- Use 'confidential' within the strapline of an internal email, to add an additional layer of encryption.

When personal data is stored on any portable computer system:

- 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 once it has been transferred or its use is complete.

7. Communications

A wide range of rapidly developing communication technologies have 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:

	Staff & other adults			Students / Pupils		
Communication Technologies	Allowed	Allowed at certain times	Allowed for selected staff	Allowed	Allowed at certain times	Allowed with staff permission
Mobile phones may be brought to school		✓				✓
Use of mobile phones in lessons						
Use of mobile phones in social time		✓				
Taking photos on mobile phones / cameras						
Use of other mobile devices eg tablets, gaming devices		✓				
Use of personal email addresses in school, or on school network						
Use of school email for personal emails						
Use of messaging apps (Class Dojo)			✓			
Use of social media			✓			
Use of blogs			✓			

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

- The official Trust 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 academy email service to communicate with others when in school, or on academy systems (eg by remote access).
- Users must immediately report to the Head of School if they receive 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 parents / carers (email, chat, ClassDojo, VLE etc) must be professional in tone and content. These communications may only take place on official (monitored) Trust 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 may be provided with an individual email address for educational use, when appropriate. All email systems will be closely monitored by academy staff.
- Students / pupils should be taught about digital safeguarding 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 Trust website and only official email addresses should be used to identify members of staff.

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

The Trust 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:

- Policies, including: acceptable use and social media protocols; 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.
- 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 academy or local authority.
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

CCE's use of social media, for professional purposes, will comply with this policy.

9. Unsuitable / inappropriate activities

The Trust 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 Trust 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
	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 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 eg Youtube			X		

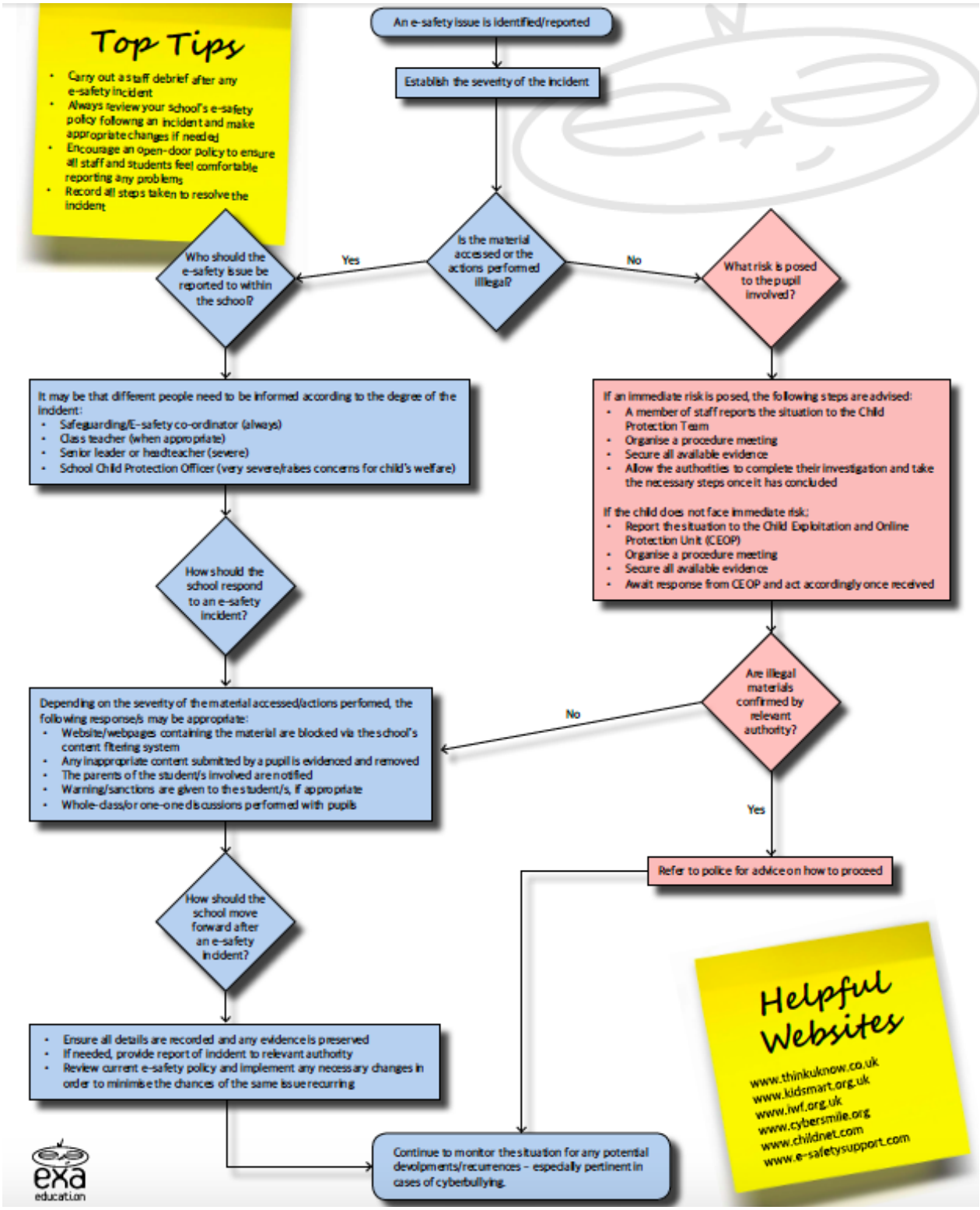
10. Prevent Duty relevance

This policy and relevant sections of this policy are to be read in conjunction with the Government's guidance and updates on the Prevent Duty. All updates within this area are taken into account when dealing with incidents of filtering breach / inappropriate actions by all users within the Academy Trust.

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/439598/prevent-duty-departmental-advice-v6.pdf

11. Responding to incidents of misuse

It is hoped that all members of the Trust community will be responsible users of digital technologies, who understand and follow Trust policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse. Please use the flow diagram below to plan the response to an incident.



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 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 recorded using the Trust incident logging system- CPOMS/My Concern.
- 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 disciplinary procedures.
    - Involvement by the Local Authority 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.
    - 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 Trust and, possibly, the police and demonstrate that visits to these sites were carried out for child protection purposes. The completed incident log should be retained by the group for evidence and reference purposes.

11.1 Academy Actions & Sanctions

It is more likely that the Trust 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. Any investigations, meetings and/or outcomes must be recorded on My Concern/CPOMS.

Students / Pupils Actions / Sanctions

Incidents:	Refer to class teacher / tutor	Refer to Head of School	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 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	X			X
Unauthorised use of non-educational sites during lessons	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	
Unauthorised downloading or uploading of files	X			X			X	
Allowing others to access academy network by sharing username and passwords	X			X				X
Attempting to access or accessing the academy network, using another student's / pupil's account	X	X		X				X
Attempting to access or accessing the academy network, using the account of a member of staff	X	X		X	X	X		X
Corrupting or destroying the data of other users	X	X		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	X			X	X		X
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	X	X			X			X
Using proxy sites or other means to subvert the school's / academy's filtering system	X			X	X	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	X	X		X
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act	X	X		X	X		X	

Staff Actions / Sanctions

Incidents:	Refer to line managerr	Refer to Head of School/ CEO	Refer to Police	Refer to Technical Support Staff for action re filtering etc	Warning	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	
Inappropriate personal use of the internet / social media / personal email	X	X		X	X	
Unauthorised downloading or uploading of files	X	X		X		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		X	X	
Careless use of personal data eg holding or transferring data in an insecure manner	X	X		X		X
Deliberate actions to breach data protection or network security rules	X	X		X		X
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	X	X		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			X
Actions which could compromise the staff member's professional standing	X	X				X
Actions which could bring the academy into disrepute or breach the integrity of the ethos of the academy	X	X				X
Using proxy sites or other means to subvert the school's / academy's filtering system	X	X		X		X
Accidentally accessing offensive or pornographic material and failing to report the incident	X	X		X		
Deliberately accessing or trying to access offensive or pornographic material	X	X		X		X
Breaching copyright or licensing regulations	X	X			X	
Continued infringements of the above, following previous warnings or sanctions	X	X				X