



E-SAFETY POLICY

Policy Reference No	IT002
Review Frequency	Annual
Reviewed	Summer 2026
Next Review Date	Summer 2027
Approved by	TLT

(This policy supersedes all previous E-Safety policies)

FLOURISHING FUTURES
Empower, Excel, Together



Change Log

Date	Changes to Policy
Summer 2026	Updates throughout to reflect our Ped Teach work on Teams and the DFE Digital Standards. Specific updated: Principles to Introduction Updated Introduction to reflect current uses of digital technologies, including links to wellbeing. Introduction: Added in legislation and guidance list Section 2: Roles and Responsibilities updated re Class Teams Section 4: updated to reflect new, more robust, 'Student Keeper' Filtering and Monitoring. Section 5: Updated Curriculum to reflect updated schemes of work and content (including new RHE Curriculum) and added section on AI to Curriculum Section 6: Added to reflect wide range of communication technologies used and that these are ever evolving. Section 7: Updated wording for UK GDPR compliance to improve clarity and align with ICO guidance, including strengthened data protection principles, staff responsibilities, and security requirements.
Spring 2026	Section 2.7 Updated to reflect Trust phone-free school day and ensure consistency across safeguarding and behaviour policies. Page 17: Actions and Sanctions Page 21: E-Safety Charter updated
September 2025	Updated introduction content in line with KCSIE 2025 e.g. mis and dis information Accessibility and Language Support added.
Spring 2024	Trust use checklist amended from mobile phones and devices with cameras to mobile phones, cameras and other electronic devices with imaging and sharing capabilities. Use of mobile phones in lessons updated to include and/ or around pupils Use of mobile phones in social time updated to include away from pupils Actions & sanctions checklist amended from mobile phones and devices with cameras to mobile phones, cameras and other electronic devices with imaging and sharing capabilities.
Autumn 2023	Updated inline KCSIE 2023: Introduction wording with 4Cs of E Safety. Section 2: roles and responsibilities of Filtering and Monitoring.
Autumn 2022	Amend Head of Academy to Head Teacher
Autumn 2022	Securly link updated page 6
Autumn 2021	Policy reviewed to reflect Managed Partnership with Computeam, infrastructure update and new Securly filtering system

Contents

Change Log.....	2
Contents.....	2
Introduction	3
1. Policy Document	4
2. Roles and Responsibilities.....	4
2.1 Trust Leadership Team	4
2.2 Head Teachers and Senior Leaders.....	4
2.3 Member of SLT with responsibility for e-safety.....	4
2.4 External ICT Support	5
2.5 Teaching and Support Colleagues	5
2.6 Designated Safeguarding Lead (DSL).....	5
2.7 Pupils	5
2.8 Parents/Carers.....	6
3. Education and Training	6
3.1 Education and Training – Colleagues.....	6
3.2 Training – Trustees	6
3.3 Education – Parents / Carers.....	6

4.	Infrastructure, equipment, filtering and monitoring	7
5.	Curriculum.....	8
6.	Use of digital and video images	10
7.	UK GDPR (UK General Data Protection Regulation)	11
8.	Communications	12
9.	Unsuitable / inappropriate activities	13
10.	Responding to incidents of misuse	15
10.1	Flowchart for responding to online safety incidents	16
Appendix 1: E-Safety – A School Charter for Action		Error! Bookmark not defined.
Our school community.....		Error! Bookmark not defined.
Appendix 2: Resources and further information		21
.....		21

Accessibility and Language Support

If you require this policy in an alternative format or language, please contact the Academy Office. We are committed to ensuring that all colleagues have access to our policies and can fully understand and engage with them and will work with you to provide the necessary support and resources.

Introduction

The following legislation and guidance has been considered when drafting this policy:

- Keeping Children Safe in Education (current year)
- Education Act 2002
- Education and Inspections Act 2006
- UK GDPR & Data Protection Act 2018
- DfE Filtering and Monitoring Standards
- Equality Act 2010

The Trust's approach to online safety is based on:

- Education rather than restriction
- Proportional risk management
- Safeguarding at the centre
- Partnership with parents/carers
- Continuous review in response to emerging technologies

The Trust recognises that the internet and digital technologies are an integral part of children and young people's lives. Used effectively, they can enhance learning, improve access to education, support communication, and promote inclusion for all pupils, including those with SEND.

However, the use of digital technologies also presents a range of risks, both inside and outside of the academy. These include exposure to harmful content, online exploitation, cyberbullying, misinformation, and risks associated with emerging technologies such as artificial intelligence (AI).

The Trust adopts a **balanced, risk-based approach** to online safety. We aim not to restrict access unnecessarily, but to educate and empower pupils to use technology safely, responsibly, and critically.

The four key areas of risk remain:

- **Content:** Exposure to harmful, inappropriate or misleading material, including misinformation, disinformation,

deepfakes, and harmful online communities.

- **Contact:** Harmful interactions with others online, including grooming, exploitation, coercion, and peer-on-peer abuse.
- **Conduct:** Online behaviour that increases risk, including bullying, harassment, sharing of images, and inappropriate use of digital platforms.
- **Commerce:** Financial risks such as scams, phishing, in-app purchases, gambling, and exploitation through digital platforms.

The Trust further recognises that digital technology can impact pupils' **mental health and wellbeing**, including through excessive use, sleep disruption, online comparison, and exposure to harmful or distressing content.

Through education, safeguarding systems, and strong partnerships with parents/carers, the Trust seeks to ensure that all pupils develop the skills, resilience, and knowledge required to navigate the online world safely.

1. Policy Document

This policy applies to all members of the Trust community (including colleagues, pupils, volunteers, parents/carers and visitors) who have access to and are users of the Trust's Digital Technologies systems and equipment, both in and out of our schools. Our PedTeach development means that we see our online communities as an extension of the physical world, including our schools and classrooms. This policy sits alongside other policies, such as Safeguarding and Acceptable User and applies to all colleagues, pupils and families. Alongside this development, there remains an expectation that all use technology safely and responsibly and that this is paramount.

The Education and Inspections Act 2006 empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of colleagues to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other e-safety incidents covered by this policy, which may take place out of the academy, but is still linked to membership of the academy. The Trust will deal with such incidents within this policy and associated behaviour and inappropriate e-safety behaviour that take place out of school. Parents/carers may be informed of concerns to ensure partnership working.

2. Roles and Responsibilities

The following section outlines the roles and responsibilities for the e-safety of individuals and groups within the Trust:

2.1 Trust Leadership Team

Trust Leadership Team are responsible for the approval of this Policy and for reviewing the effectiveness of the policy as well as the annual review of the Monitoring and Filtering System.

2.2 Head Teachers and Senior Leaders

- Chief Executive Officer and Head Teacher are responsible for ensuring the safety (including e-safety) of members of their academy communities;
- Chief Executive Officer, Head Teacher and senior leaders are responsible for ensuring that relevant colleagues receive suitable training and development to enable them to carry out their e- safety roles and to train other colleagues, as relevant;
- Chief Executive Officer, Head Teacher and senior leaders will ensure that there is a system in place to allow for the monitoring and support of those in the school who carry out the internal e-safety monitoring role, such as Designated Safeguarding Leads (DSL). This is to provide a safety net and also to support those colleagues who take on important monitoring roles;
- Each academy's senior leadership team (SLT) will receive information regarding any e-safety incidents by the DSL. These incidents include those highlighted to the DSL by the 'Student Keeper' safety and security application. These will be logged and reviewed during SLT meetings;
- Chief Executive Officer, Head Teacher and members of each academy SLT should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of colleagues or pupil.

2.3 Member of SLT with responsibility for e-safety

- Take day to day responsibility for e-safety issues and oversee the sanctions for breaches of rules relating to e-safety;
- Ensure that all colleagues are aware of the procedures that need to be followed in the event of an e-safety incident taking place;

- Provide training and advice to colleagues through annual at least annual training as well as at Induction.
- Liaise with the Local Authority Designated Officer (LADO) or Police as appropriate;
- Liaise with the Trust's external ICT technical consultants (Computeam)
- Receive reports of e-safety incidents from in school DSL as part of behaviour monitoring;
- Provide information to the Trust Leadership Team/Board as appropriate.

2.4 External ICT Support

- Ensure that the academy and Trust ICT infrastructure is secure and is not open to misuse or malicious attack and that all aspects of the Trust's ICT systems are secure, in line with the Trust's guidance and policies.
- Filtering and Monitoring service is live and runs 24 hours a day, 7 days a week.
- Live support from the ICT Consultants (Computeam) is available 8.00-5.30pm
- Ensure that appropriate alerting and reporting is in place to Trust DSL colleagues at all times.

2.5 Teaching and Support Colleagues

Teaching and support colleagues are responsible for ensuring that:

- They have an up-to-date awareness of e-safety matters and of current Trust e-safety policy and practices;
- They have had training on and understand the schools monitoring and filtering system and how to raise concerns with the DSL.
- They have read and understood the appropriate ICT agreements;
- They report any suspected misuse or problem to a member of SLT;
- Digital communications with pupils are only on a professional level and carried out using official Trust systems;
- It is understood that social media can play an important part in communication between the Trust and pupils, parents/carers; however, there is also a need to ensure it is used in an appropriate and safe way.
- E-safety issues are embedded in all aspects of the curriculum and other academy activities;
- Pupils understand and follow the Trust's E-safety and Acceptable Use Policy;
- Pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations;
- They monitor ICT activity in lessons, extra-curricular and extended academy activities;
- They are aware of e-safety issues related to the use of mobile phones, cameras and hand-held devices and that they monitor their use and implement current best practice with regard to these devices;
- In lessons where internet use is pre-planned, pupils should be guided to sites that are checked as suitable for their use and that processes are in place to deal with any unsuitable material that is found in internet searches.
- Colleagues must not use AI tools to process or enhance images of pupils unless this has been explicitly approved and risk assessed via the AI Tools Approval process.

Class Teams is an important tool for teaching and learning. There are safeguards in place, and pupils and colleagues have training to support them to use this technology responsibly.

- The 'Chat' function is not available to children under this usage.
- Pupils may be set Assignments and Notebooks in school and may respond by 'handing in work' or writing a 'Post'.
- Pupils 'use of 'Posts' must be muted as standard, and only 'unmuted' during specific lessons where they are using Class Teams under supervision. Class teachers are responsible for this.
- Class Teams will be used to support learning in school, under the supervision of colleagues, and is not used outside of school. E.g. as Home Learning.

2.6 Designated Safeguarding Lead (DSL)

Are trained in the use of the Trust safety and security tools (Filtering and Monitoring-Student Keeper) They are also responsible to address all issues that are alerted to them by the Student Keeper software as well as ensuring colleagues understand the system and their wider role within it.

DSL colleagues should be trained in e-safety issues and be aware of the potential for serious child protection 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

2.7 Pupils

- Are responsible for using the Trust's ICT systems in accordance with Trust policy, which they will be expected to sign for before being given access to the Trust systems;

- 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 that the Trust operates a phone-free school day for pupils as part of its safeguarding approach and follow the Trust's policies relating to mobile phones and personal smart devices
- If there is an agreement in place mobile phones must be handed in at the beginning of the day for secure storage
- They should also know and understand the Trust's policies on the taking/use of images, include manipulation, altering of images including cyber-bullying.
- Should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the Trust E-Safety Policy covers their actions out of the school, if related to their membership of the Trust.

2.8 Parents/Carers

Parents/carers play a crucial role in ensuring that their children understand the need to use the internet/digital technologies in an appropriate way. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of ICT than their children. The Trust will therefore take every opportunity to help parents understand how to support their children in making safe choice and use of such technologies.

Parents/carers and volunteers will be responsible for:

- Endorsing the Trust policy;
- Accessing the academy website in accordance with the relevant Acceptable Use Policy.
- Supporting their children to use digital technologies safely.

3. Education and Training

E-Safety education will be provided to pupils in a range of ways. These include the planned Computing and Relationships and Health Education curriculums, Assemblies and wider school activities. More information on this is in the Curriculum Section.

3.1 Education and Training – Colleagues

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

- The use of the Student Keeper filtering and security platform
- E-safety training for all colleagues is undertaken on an annual basis. Further e-safety training will be included as part of colleagues's child safeguarding training;
- All new colleagues will receive e-safety training as part of their induction programme, ensuring they understand the E-safety Policy, Cyber Security, Prevent and Safeguarding and Acceptable Use Policy.

3.2 Training – Trustees

The Trust's annual Child Safeguarding and Prevent training covers the relevant elements of e-safety training. Trustees are required to undertake the Trust's Safeguarding Children and Prevent Training on an annual basis.

3.3 Education – Parents / Carers

Parents' confident, knowledge and understanding of use, benefits and risks of the Internet and Digital Technologies, may vary a great deal. It is recognised the highly important role that parents have in supporting, monitoring and regulating their children's use of the Internet and digital technologies. Parents often either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it. "There is a generational digital divide". (Byron Report).

The school will therefore seek to provide information and awareness to parents and carers in a range of ways. This includes offering an Annual Workshop and follow-up resource (during Internet Safety Week). In addition to this, schools will regularly communicate updates to families, including being responsive to emerging trends or technologies. These may include:

- Letters, newsletters, web site updates
- Parents evenings or open sessions
- Reference to websites such as the SWGfL Safe website (nb the SWGfL "Golden Rules" for parents), ThinkuKnow, Torbay Virtually Safe, Devon.gov.uk

4. Infrastructure, equipment, filtering and monitoring

The Trust will be responsible for ensuring that the school's infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented.

- All users will have clearly defined access rights to Trust's ICT systems;
- All colleagues users will be provided with a username and password by ICT support who will keep an up-to-date record of users and their usernames. Users will be required to change their password regularly;
- All pupil users will be provided with a username and password by (systems manager) who will keep an up-to-date record of users and their usernames. Users will learn how to change their password regularly as part of their curriculum learning.
- Users will be made responsible for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security;
- In the event that the filtering and security system needs to be 'restarted' or 'switched off' for any reason, or for any user, this must be logged and carried out by a process that is agreed by the Head Teacher or Chief Executive Officer;
- Requests from colleagues for sites to be removed from the filtered list must be addressed through the schools DSL who will have the system 'rights' to make any agreed changes.
- ICT technical Consultants (Computeam) regularly monitor and record the activity of users on the Trust's ICT systems and users are made aware of this in the Acceptable Use Policy;
- Remote management tools are used by colleagues to control workstations and view users' activity;
- An appropriate system is in place for users to report any actual / potential e- safety incident to SLT;
- Appropriate security measures are in place to protect the Trust wide ICT solution from accidental or malicious attempts which might threaten the security of the Trust's systems and data;
- The "master / administrator" passwords for the Trust ICT solution, must also be available to the Chief Executive Officer or other nominated senior leader and kept in a secure facility at Trust Head Office.
- Guest users and visiting professionals can securely access the internet utilising wireless connectivity;
- Personal use of the Trust's ICT systems should be limited to what may be deemed reasonable. The services are provided predominantly for education purposes;
- Neither colleagues nor pupils should install programmes or other software on workstations, portable devices. If any programme / application needs loading onto the Trust wide ICT system then this should be logged as a 'ticket' and will be addressed by the ICT provider.;
- Each academy's ICT infrastructure and individual workstations are protected by up-to-date virus software;
- Personal data (as defined by the Data Protection Act) cannot be sent over the internet or taken off the academy site unless safely encrypted or otherwise secured by password or other;
- Where colleagues have email accounts and other Trust data on their phone or other mobile device they must ensure that the device is locked with a password.

In addition to the points below the following link is to the Securly IWF (Internet Watch Foundation) Accreditation page:
[Securly | IWF Membership | IWF](#)

The Trust will ensure that appropriate filtering and monitoring systems are in place to safeguard pupils and colleagues.

- **Filtering systems** are used to restrict access to harmful or inappropriate content
- **Monitoring systems** are used to identify and respond to safeguarding concerns, including indicators of risk such as self-harm, bullying, or exploitation

Monitoring systems:

- Provide alerts to trained safeguarding colleagues (DSLs)
- Are regularly reviewed for effectiveness
- Do not replace the need for colleagues vigilance and professional judgement

All concerns identified through monitoring systems will be reviewed and acted upon in line with safeguarding procedures.

Ipads

Ipads or other devices (which do not have individual log ins), must have robust physical monitoring. This means that adults must be continually supervising their use. It is not recommended that Ipads are used for large group or whole class work, for this reason. Schools may wish to assign logs in for up to 5 pupils per Ipad with Computeam- this is the maximum recommended number per Ipad.

5. Curriculum

Online safety education will be embedded across the curriculum and reinforced through the Computing Curriculum, Relationship and Health Education (via OAK Academies), assemblies and wider school activities.

Pupils will be taught to:

- Use digital technologies safely, responsibly and respectfully
- Critically evaluate online content, including identifying misinformation, disinformation and deepfakes
- Understand how algorithms and online platforms (e.g. social media, video-sharing platforms) influence the content they see
- Recognise and respond to online risks, including grooming, exploitation, bullying and scams
- Understand the risks associated with sharing personal information and images online
- Use AI and emerging technologies responsibly and critically
- Respect intellectual property, copyright and academic integrity

Teaching will also address modern online behaviours and risks, including:

- Use of social media platforms, messaging apps and group chats
- Online peer pressure and harmful trends
- Livestreaming and gaming environments
- Digital wellbeing, including screen time, sleep and mental health

Pupils will be encouraged to report concerns and seek support. They will be reassured that they will be taken seriously and supported appropriately.

6. Use of Artificial Intelligence (AI) and Emerging Technologies.

The Trust recognises the increasing use of artificial intelligence (AI) and other emerging technologies in education and daily life.

Opportunities

AI tools can support:

- Adaptive and personalised learning
- Accessibility (e.g. translation, reading support)

- Colleagues workload reduction (planning, feedback, administration)

Risks

However, AI presents new safeguarding and educational risks, including:

- Inaccurate or misleading information (“hallucinations”)
- AI-generated misinformation and deepfake images, audio, or video
- Academic integrity concerns, including AI-assisted plagiarism
- Data protection risks where personal information is shared with AI tools
- Potential for inappropriate or harmful interactions with AI chatbots

Expectations

- Colleagues must adhere to the Trust AI Policy, which sets out how AI must be used **safely, ethically, and critically**
- AI-generated content must not be assumed to be accurate and should be verified
- AI must not be used to bypass learning or assessment expectations unless explicitly permitted
- Personal or sensitive data must not be shared with AI tools.

The Trust has been supported by ICT Technology Consultants (Computeam) in the development of its AI Policy and provides guidance and training to colleagues on the appropriate use of AI technologies. This guidance has due regard to DFE guidance and training for those who lead this area.

The Trust is considering the development of Pupil use of AI and will communicate any such developments with parents.

6. Digital Wellbeing

The Trust recognises that pupils’ use of digital technology can impact their wellbeing.

Pupils will be supported to understand:

- The importance of balancing online and offline activity
- The impact of screen time on sleep, concentration and mental health
- The effects of social media, including comparison culture and online validation
- Strategies to manage their digital use positively and safely

Colleagues will be alert to concerns relating to digital wellbeing and will respond in line with safeguarding and support systems.

7. Communications

The Trust recognises that communication technologies continue to evolve. This includes the use of:

- Messaging platforms (e.g. WhatsApp, Snapchat)
- Social media platforms (e.g. TikTok, Instagram)
- Gaming communication (e.g. Discord, in-game chat)

- Livestreaming platforms
- Teams as a teaching platform in schools

These platforms may present safeguarding risks, particularly where communication is unmonitored or anonymous.

The Trust's principle is that **digital communication between colleagues and pupils must only take place via approved, secure and monitored systems.**

7. Use of digital and video images

The development of digital imaging technologies has created significant benefits for teaching and learning. Colleagues and pupils can capture, use and share images to support educational outcomes. However, the use of images also presents safeguarding, data protection and reputational risks, particularly in the context of emerging technologies such as artificial intelligence (AI).

The Trust is committed to ensuring that all use of images is safe, lawful, proportionate and respectful.

6.1 General Principles

- The use of images must always support educational purposes and uphold the dignity and safety of pupils.
- All images of pupils are considered **personal data** and must be processed in accordance with UK GDPR and the Data Protection Act 2018.
- Images must be handled securely and only retained for as long as necessary.
- Colleagues must be aware that images shared online may remain accessible indefinitely and may be reused or altered without consent.

6.2 Taking and Using Images

- Colleagues may take digital or video images to support educational aims, but **only using Trust-approved devices.**
- Personal devices must not be used to take, store, or share images of pupils.
- Care must be taken to ensure:
 - Children must not be identifiable, no full faces
 - Pupils are appropriately dressed
 - Images do not place pupils at risk or bring individuals or the Trust into disrepute
- Pupils must not take, use, share, publish or distribute images of others without permission.
- Pupils will be educated about the risks associated with sharing images online, including misuse, permanence and reputational harm.

6.3 Storage, Sharing and Publication

- Images must be stored securely on Trust systems and not on personal devices or unapproved platforms.
- Photographs published externally (e.g. website, social media) will:
 - Be carefully selected
 - Not include pupils' full names
 - Comply with the Trust's Photography and Video Consent and Storage Policy
- Written parental/carer consent must be obtained before publishing images of pupils.

6.4 Use of Artificial Intelligence (AI) in Relation to Images

The Trust recognises that AI technologies can generate, edit and manipulate images in ways that increase safeguarding and data protection risks, including the creation of synthetic or "deepfake" content.

To protect pupils:

- **Images of pupils must not be uploaded to AI tools or platforms** (including image generators, editors, enhancers or similar technologies) unless:
 - The tool has been formally approved by the Trust
 - A data protection impact assessment (DPIA) has been completed
 - Appropriate safeguards are in place
- Colleagues must **not use AI tools to modify, enhance or alter images of pupils**, including:
 - Changing appearance
 - Altering context or setting
 - Generating composite or synthetic images
- AI must not be used to:
 - Create images that **represent or resemble real pupils**
 - Generate fictional or simulated versions of identifiable individuals
- Images must not be processed using AI tools that:
 - Retain, reuse, or train on uploaded data
 - Store data outside approved Trust systems without safeguards

6.5 Safeguarding and Risk Awareness (Including AI Misuse)

- All users must understand that images can be:
 - Copied, shared or altered without consent
 - Used inappropriately or maliciously, including through AI technologies
- Pupils will be taught about risks including:
 - Image sharing and consent
 - Online exploitation and misuse
 - AI-generated manipulation (e.g. deepfakes)
- Any concerns regarding misuse of images must be reported immediately in line with safeguarding procedures.

6.6 Accountability and Compliance

- Colleagues are responsible for ensuring that all image use complies with:
 - This policy
 - The Trust's Data Protection Policy
 - The Trust's AI Policy
- Breaches of this section may be treated as a safeguarding concern and/or data protection incident and managed through appropriate procedures.

8. UK GDPR (UK General Data Protection Regulation)

Personal data will be processed in accordance with UK GDPR and the Data Protection Act 2018.

The following data protection principles are applied at all times:

- Personal data shall be processed lawfully, fairly and in a transparent manner.
- Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner incompatible with those purposes.
- Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (data minimisation).
- Personal data shall be accurate and, where necessary, kept up to date.
- Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary (storage limitation).
- Personal data shall be processed in a manner that ensures appropriate security, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage (integrity and confidentiality).
- We are responsible for, and must be able to demonstrate, compliance with these principles (accountability).

Colleagues must ensure that they:

- Take all reasonable steps to ensure the secure handling and safekeeping of personal data, minimising the risk of loss or misuse;
- Access and process personal data only on secure, password-protected systems and devices;
- Log off systems when not in use;
- Transfer personal data securely, using encryption or password protection where appropriate

When personal data is stored on portable devices (e.g. laptops, tablets, USB devices)

- The data must be encrypted and password protected;
- The device must be password protected;
- The data must be securely deleted once it is no longer required.

Particular care must be taken when processing images or media, as these may be subject to unauthorised sharing or misuse, including through emerging technologies such as artificial intelligence (AI).

Photographic images of pupils are personal data and must be treated accordingly.

This includes ensuring that:

- Images are not uploaded to third-party AI systems without approval
- Images are not processed using tools that retain, train on, or reuse data
- Appropriate safeguards are in place to prevent unauthorised reuse or manipulation

9. Communications

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

	Colleagues & other adults				Pupils			
Communication Technologies	Allowed	Allowed at certain times	Allowed for selected colleagues	Not allowed	Allowed	Allowed at certain times	Allowed with colleagues permission	Not allowed
Mobile phones, cameras and other electronic devices with image sharing capabilities, may be brought to school.	X						X	
Use of mobile phones and other electronic devices with image sharing capabilities, may be brought to school in lessons and/ or around pupils.				X				
Use of mobile phones in social time (away from pupils).	X							X
Taking photos on Trust mobile phones, cameras or other electronic devices with image sharing capabilities.		X					X	
Use of Trust devices eg PDAs, Laptops	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 Class Teams: Assignments, Notebook and Posts.		X					X	
Use of Class Teams Chat				X				X
Use of social networking sites		X						X

The Trust considers the following as good practice:

- The official Trust email service may be regarded as safe and secure and is monitored. Colleagues should therefore use only the academy email service to communicate with others when in school, or on school systems (e.g. by remote access).
- Users need to be aware that email communications are monitored
- Users must immediately report to the nominated person – in accordance with the Trust policy, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.
- Any digital communication between colleagues and pupils or parents / carers (email, chat, Class Teams etc) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or public chat / social networking programmes must not be used for these communications.
- Pupils should be taught about email safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of colleagues.
- The use of educational streaming video clips such as YouTube is acceptable. Videos should be checked prior to screening by an adult. The video should be documented prior to the lesson and not allowed to auto run into the next video. Videos should be shown in full screen so to minimize any comments surrounding the video. Pupils should be fully supervised if watching any clips.

9. Unsuitable / inappropriate activities

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and is obviously banned from the Trust and all other ICT systems. Other activities e.g. Cyber-bullying, use of electronic communications to radicalise children or others, is 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. School policy restricts certain internet usage as follows:

User Actions	Acceptability	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				X
	promotion or conduct of illegal acts, eg under the child protection, obscenity, computer misuse and fraud legislation				X
	adult material that potentially breaches the Obscene Publications Act in the UK				X
	criminally racist material in UK				X
	pornography				X

	promotion of any kind of discrimination				X
	promotion of racial or religious hatred				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	
Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the Trust				X	
Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions				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	
Carrying out sustained or instantaneous high volume network traffic (downloading / uploading files) that causes network congestion and 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 networking sites		X			
Use of video broadcasting e.g. YouTube.		X			
The use of on demand film sites such as Netflix, Amazon, Now TV and Disney Life in schools when using a personal account.					X
The downloading & storage of video clips e.g. YouTube clips					X

10. Responding to incidents of misuse

It is hoped that all members of the school community will be responsible users of ICT, who understand and follow this policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse. Listed below are the responses that will be made to any apparent or actual incidents of misuse:

If any apparent or actual misuse appears to involve illegal activity, i.e.:

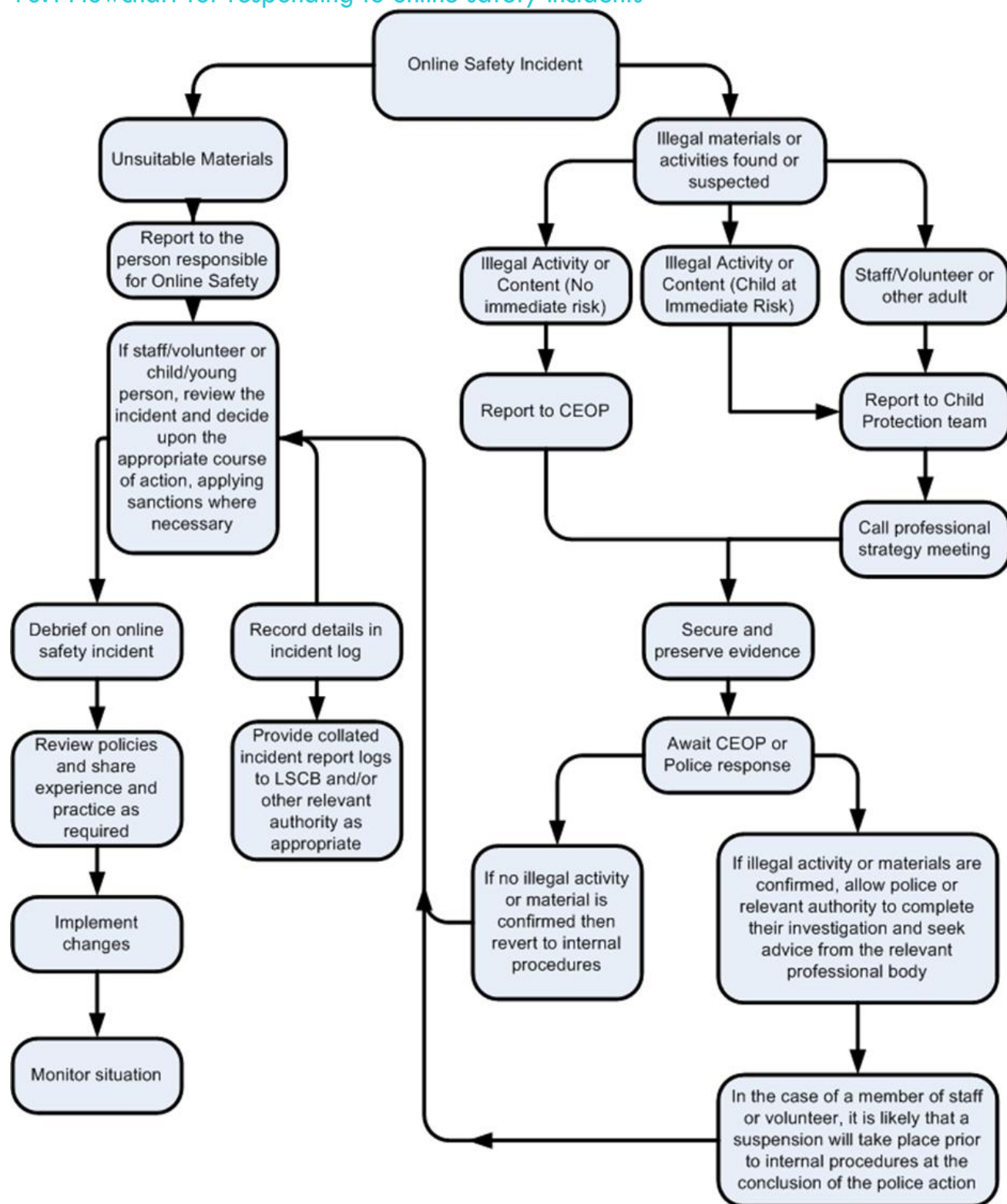
- child sexual abuse images
- adult material which potentially breaches the Obscene Publications Act
- criminally racist material
- other criminal conduct, activity or materials

Remove pupils, colleagues and others from exposure to the material and immediately notify the Chief Executive Officer (or nominated individual in her absence) who should then contact the police. Further action should be agreed with the police.

If members of colleagues suspect that misuse might have taken place, but that the misuse is not illegal (as above) it is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation. In such event the SWGfL "Procedure for Reviewing Internet Sites for Suspected Harassment and Distress" should be followed. This can be found on the SWGfL Safe website within the "Safety and Security booklet". This guidance recommends that more than one member of colleagues is involved in the investigation which should be carried out on a "clean" designated computer. (see flow chart below for this)

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 behaviour / disciplinary procedures as follows:

10.1 Flowchart for responding to online safety incidents



Pupils	Actions / Sanctions								
Incidents:	Refer to class teacher / tutor	Refer to Head Teacher	Refer to Chief Executive Officer	Refer to Police	Refer to DSL for action re filtering / security etc	Inform parents / carers	Removal of network / internet access rights	Warning	Further sanction e.g. 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	X	X	
Unauthorised use of non-educational sites during lessons	X				X			X	
Mobile phones, cameras and other personal electronic devices with image-sharing capabilities are not permitted to be brought into school by pupils, unless explicitly agreed in advance for safeguarding or medical reasons.	X	X			X	X		X	
Unauthorised use of social networking / instant messaging / personal email	X	X			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	X				X		X	X	
Attempting to access or accessing the school network, using another pupil's account		X			X	X	X	X	
Attempting to access or accessing the school network, using the account of a member of colleagues		X			X	X	X	X	
Corrupting or destroying the data of other users		X			X	X	X	X	
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature		X			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	X		X

Using proxy sites or other means to subvert the school's filtering system		X			X	X	X	X	
Accidentally accessing offensive or pornographic material and failing to report the incident	X	X			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	

Colleagues	Actions / Sanctions							
Incidents:	Refer to Head Teacher	Refer to Chief Executive Officer	Refer to Local Authority / HR	Refer to Police	Refer to DSL for action re filtering / security etc	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	X		X	X
Excessive or inappropriate personal use of the internet / social networking sites / instant messaging / personal email	X				X	X		
Unauthorised downloading or uploading of files	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		
Careless use of personal data e.g. holding or transferring data in an insecure manner	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 instant message that is regarded as offensive, harassment or of a bullying nature	X	X			X		X	X
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with pupils	X	X			X	X	X	X
Actions which could compromise the colleagues member's professional standing	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 filtering system	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
Breaching copyright or licensing regulations	X	X			X	X		
Continued infringements of the above, following previous warnings or sanctions	X	X			X		X	X

Appendix 2: Resources and further information

Devon County Council, Online Safety for Education and Families: <https://www.devon.gov.uk/eycs/providers/safeguarding/online-safety/>

Torbay Safeguarding Children Partnership: <http://torbaysafeguarding.org.uk/cyp/online-safety/>

Practical online safety advice for people in Torbay which aims to keep children safer online:
<http://www.torbayvirtuallysafe.co.uk/>

NSPCC: <https://learning.nspcc.org.uk/research-resources/schools/e-safety-for-schools/>
<https://www.nspcc.org.uk/keeping-children-safe/online-safety/>

Think U Know: <https://www.thinkuknow.co.uk/>

SWGFL: <https://swgfl.org.uk/>