December 2023

TCAT Primary Schools

E-Safety Policy

SERVE CHALLENGE EMPOWER

Document Control

Primary Member Academies:	Appleton Thorn Primary School (ATP) Broomfields Junior School (BRO) Great Sankey Primary School (GSP) Meadowside Community Primary and Nursery School (MEA) Penketh South Primary School (PSP)

Version	**Date**	**Action**
1	**	Drafted by the Trust Head of IT and approved by the Operations Director, Director of Education, TCAT Safeguarding Lead, Headteachers
2		
3		
4		

Table of Contents

1.0 Introduction.....4

2.0 Objectives.....5

3.0 Roles & Responsibilities.....6

4.0 E-Safety Education.....9

5.0 Digital Devices.....12

6.0 Online Content Filtering.....13

7.0 Responding to incidents of misuse.....16

1.0 Introduction

This E-safety policy outlines the guidelines, procedures, and responsibilities to ensure the safe and responsible use of digital technologies and the internet within The Challenge Academy Trust (TCAT) and all of the Primary schools within the Trust.

The policy aims to safeguard our young people, staff, and the wider school community from potential online risks and to promote a positive digital learning environment.

This E-Safety policy applies to all members of the TCAT Primary school community and incorporates the following (including staff, temporary staff, Initial Teacher Training staff, young people both nursery and primary, volunteers, parents/carers, visitors, community users, leisure users and Governors) who have access to and are users of school network and management systems both in and out of school.

This includes all web based TCAT and Primary school branded websites, intranets, cloud resources, social media accounts and marketing areas.

The Education and Inspections Act 2006 empowers Principals to such extent as is reasonable, to regulate the behaviour of young people when they are off the Primary school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of online bullying or other online safety incidents covered by this policy, which may take place outside of the TCAT primary school, but is linked to membership of the TCAT primary school. TCAT Primaries will work with parents/carers to manage incident of online bullying which take place outside of the setting.

This E-Safety Policy should be read in line with the following other policies:

Keeping Children Safe in Education and alongside each settings:
Safeguarding and Child Protection Policy
Behaviour Policy
Acceptable Use Policy

2.0 Objectives

Our e-safety policy seeks to achieve the following objectives:

Educate young people about safe and responsible online behaviour.

Protect young people from exposure to harmful and inappropriate content.

Prevent cyberbullying, harassment, and other forms of online misconduct.

Safeguard personal information and privacy.

Promote the ethical use of technology and respect for intellectual property.

Provide guidelines for staff in facilitating safe online experiences.

Establish procedures for dealing with e-safety incidents.

3.0 Roles and Responsibilities

The following section outlines the E-Safety roles and responsibilities of individuals within TCAT Primary schools:

3.0 TCAT – The Trust are responsible for the creation, adaption and review of this policy for all TCAT Primary schools. To support the integration of this policy into the school environment.

3.1 Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about E-Safety incidents and monitoring reports. A member of the Governing Body has taken on the role of Safeguarding Governor (as part of the Child Protection Governor role). The role of the Safeguarding Governor will include:

- regular meetings with the Safeguarding Team
- regular monitoring of E-Safety incident logs (generic logs)
- regular monitoring of filtering / change control logs (generic logs)
- reporting to relevant Governors / committees

3.2 The TCAT Primary School Headteacher has a duty of care for ensuring the safety (including E-Safety) of members of the school community, though the day to day responsibility for E-Safety will be delegated to the Safeguarding Team.

3.3 The TCAT Primary School Headteacher and (at least) another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious e- safety allegation being made against a member of staff.

3.4 The Headteacher / Senior Leaders are responsible for ensuring that the Designated Safeguarding lead and other relevant staff receive suitable training.

3.5 The Headteacher / Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal E-Safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.

3.6 The Senior Leadership Team will receive regular monitoring reports from the Trust of matter relating to E-Safety.

3.7 The IT Provider (Abtec) is responsible for ensuring:

- that the school's technical infrastructure is secure and is not open to misuse or malicious attack to the best of their knowledge.
- that TCAT Primary schools meets required E-Safety technical requirements and any other relevant body E- Safety Policy / Guidance that may apply and any supplementary policies to this.
- 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 is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person.
- work closely with filtering and security provider to ensure the latest filtering and protection methods are applied to the firewall and filtering software.
- that they keep up to date with E-Safety technical information in order to effectively carry out their e- safety role and to inform and update others as relevant.
- that the use of the network / internet / Microsoft/Google and clouds services / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Headteacher; E-Safety Coordinator for investigation / action / sanction.

3.8 Teaching and Support Staff are responsible for ensuring that:

- they have an up to date awareness of E-Safety policies and procedures and the current and latest E-Safety practices.
- they have read, understood and signed the Staff Acceptable Use Policy / Agreement (AUP)
- they report any suspected misuse or problem to the safeguarding lead for investigation / action / sanction.
- all digital communications with pupils / parents / carers should be on a professional level and only carried out using official school systems.
- E-Safety issues are embedded in all aspects of the curriculum and other activities
- Young people understand and follow the E-Safety and acceptable use policies.
- Young people have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- they monitor network activity in lessons, extra-curricular and extended school activities using school approved systems.
- in lessons young people are guided with the use of the Internet by the Teachers/Support teacher within the class to suitable pages and safe search results.
- take personal responsibility for their professional development in this area.

3.9 Child Protection / Safeguarding Designated Person (TCAT Safeguarding Hub)

Should be trained in E-Safety issues, including PREVENT, and be aware of the potential for serious child protection / safeguarding issues to arise from, but not limited to:

- online safety which, amongst other things, includes an understanding of the expectations, applicable roles, and responsibilities in relation to filtering and monitoring
- abuse which can take place wholly online, or technology which may be used to facilitate offline abuse
- sharing of personal data
- access to illegal / inappropriate materials
- inappropriate on-line contact with adults / strangers
- potential or actual incidents of grooming
- cyber-bullying
- child on child abuse
- extremism / radicalisation
- preventing people from becoming involved in, or supporting, terrorism
- self-harm
- sexting
- sexual abuse
- hazing / initiations / online challenges
- child criminal exploitation / child sexual exploitation

3.10 Young People/Learners

- are responsible for using TCAT primary schools digital technology systems in accordance with the man/Learners 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 using school approved systems
- will be expected to know and understand policies on the use of mobile/tablet devices/digital cameras/Smart Phone/Smart Watches
  They should also know and understand policies on the taking / use of images and on cyber-bullying.
- should understand the importance of adopting good E-Safety practice when using digital technologies out of school and realise that the School's E-Safety Policy covers their actions out of school, if related to their membership of the school.
- understand the E-Safety implications of taking and sharing personal data on social media or via the internet in general.

3.11 Parents / Carers

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, local e- safety campaigns / literature and particularly a wealth of information on the school website available at all times. Parents and carers will be encouraged to support the school in promoting good E-Safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events.
- access to parents' sections of the website/ Microsoft/Google sites and social media pages.
- their children's personal devices in the school (where this is allowed) and fully understand the rules around the use of personal devices within school
- modelling appropriate uses of new and emerging technology.
- liaising with school if they suspect, or have identified, that their Child is conducting risky/hateful/ inappropriate behaviour online.

3.12 Community/Leisure User Responsibilities

Community/Leisure Users who access any TCAT buildings or systems both on-premise and within the cloud networks or its affiliated systems as part of Extended School provision will be expected to sign the Staff Acceptable Use Policy before being provided the access to the network.

4.0 E-Safety Education

4.1 Young People

Whilst regulation and technical solutions are very important, their use must be balanced by educating young people within TCAT Primary schools to take a responsible approach. The education of young people in E-Safety is therefore an essential part of the school's E-Safety approach and provision. Children and young people need the help and support of the school to recognise and avoid e- safety risks and build their resilience and realise the risks a lack of relevant E-Safety education brings.

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

- A planned E-Safety curriculum should be provided as part of Computing (with the involvement of PHSE/ other lessons) and should be regularly revisited.
- Key E-Safety messages should be reinforced as part of a planned programme of assemblies and pastoral activities with real life examples where possible.
- Young People should be taught in all lessons to be critically aware of the materials/ content they access on-line.
- Young People should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- Young people should be helped to understand the need for the Student/Learner Acceptable Use Agreement and encouraged to adopt safe and responsible use not only at TCAT Primary schools but at home and in their general life.
- Staff should act as in an advisory capacity in their use of digital technologies the internet, social media and mobile devices.
- In lessons where internet use is pre-planned, it is best practice that Young People should be guided to sites pre checked by Teaching staff and are fit for purpose and suitable for the Year group they are Teaching.
- Where Young People are allowed to search the internet, staff should be vigilant in monitoring the content of all websites the young people visit.
- It is accepted that from time to time, for good educational reasons, young people may need to research topics (e.g. racism, drugs, discrimination, extremism, sexting, hatred etc) that would normally result in internet searches being blocked. In such a situation, firstly staff are advised to find the relevant information on another site but if this is not possible staff can request that the Technical Staff (or other relevant designated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so should be auditable, with clear reasons for the need.

4.2 Education – parents / carers

Parents 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/social media and may need advice on how to deal with a situation.

The TCAT primary schools will therefore seek to provide information and awareness to parents and carers through:

- Curriculum activities
- Letters, newsletters
- Comprehensive information the school website
- Parents / Carers evenings / sessions
- High profile events / campaigns e.g. Safer Internet Day
- Reference to the relevant web sites / publications e.g.

www.saferinternet.org.uk/

http://www.childnet.com/parents-and-carers

4.3 Staff Teaching and Support

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

- A planned programme of formal E-Safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the E-Safety training needs of all staff will be carried out regularly. It is expected that some staff will identify E-Safety as a training need within the appraisal / performance development process.
- All new staff should receive E-Safety training as part of their induction programme, ensuring that they fully understand the school E-Safety policy and Acceptable Use Agreements.
- The Safeguarding lead (or other nominated person) will receive regular updates through attendance at external training if available.
- This E-Safety policy and its updates will be presented to and discussed by staff in staff meetings / INSET days.

4.4 Training – Governors

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

- Attendance at training provided by TCAT/Local Authority / National Governors Association / or other relevant organisation.
- Participation in school training / information sessions for staff or parents.

4.5 Education – The Wider Community

TCAT can provide opportunities for local community groups / members of the community to gain from the Trust E-Safety knowledge and experience. This may be offered through the following:

- Providing family learning courses in use of new digital technologies, digital literacy and E-Safety.
- E-Safety messages targeted towards grandparents and other relatives as well as parents.
- The schools individual website will provide E-Safety information for the wider community.

5.0 Digital devices

The school and IT Provider will be responsible for ensuring that the school 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 E-Safety responsibilities:

- TCAT primary school technical systems will be managed in ways that ensure that the school meets recommended technical requirements.
- There will be regular reviews and development including audits of the safety and security of school technical systems.
- Servers, wireless systems and cabling must be securely located and physical access restricted via door locks and keypad control.
- All users will have clearly defined and relevant access rights to school technical systems and devices.
- The IT Provider (Abtec) 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 is filtered by the IT provider filtering via the firewall. Content lists are regularly updated and internet use is logged and regularly monitored. TCAT Primary schools also have a robust and secure onsite Firewall system which can provide a various comprehensive lists of banned and enabled websites, this is differentiated between staff, young people year group dependant level filtering both on the wired and wireless infrastructure.
- The IT provider and TCAT primary school regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement.
- An appropriate system is in place for users to report any actual / potential technical incident /security breach to the relevant person, as agreed.
- Appropriate security measures are in place to protect the servers, firewalls, routers, VOIP phone system, wireless networks, work stations, mobile devices and cloud based systems and online platforms such as Microsoft 365/Google Workspace including AI technology from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The TCAT primary schools 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" (e.g. trainee teachers, supply teachers, visitors) onto the TCAT Primary school systems and the access levels they are entitled to.

- An agreed policy is in place regarding the extent of personal use that users (staff / pupils / community users) can use TCAT primary school devices away from school premises.
- An agreed policy is in place that forbids staff from downloading executable files and installing programmes on school devices with the exception of Staff laptop's, this is covered in the Staff Laptop Loan Agreement.
- An agreed policy is in place regarding the use of removable media (e.g. memory sticks / CDs / DVDs) by users on school devices.
- Social Media particularly through approved TCAT school accounts is closely monitored and only available for staff to use and comment on.
- The school use of Cloud based technology is closely monitored and all emails/ communications with young peopleis reported and auditable.
- Data that is present on Cloud based systems should be treated exactly the same as data onsite that is highly sensitive and needs to be kept very secure, careful consideration should be taken when offering to share personal data across Cloud systems.
- Cloud data is still the property of the TCAT primary school it pertains to, while it may not sit on the physical school premises it is to be treated in exactly the same manner as the data which resides on the physical site.
- All TCAT primary school email is now hosted in the Cloud with Microsoft and Google.
- You must not store any sensitive school information in a cloud service which has not been formally recognised, assessed and approved by the any TCAT primary school.

6.0 Online Content Filtering

The filtering of internet content provides an essential means of preventing users from accessing material that is illegal or is inappropriate in an educational context. TCAT provide the same internet provision across all academy Primary schools, this is provided by Abtec Computers Solutions Ltd and is a 1GB dedicated 1:1 uncontended Lease line which plugs directly into the Firewall.

Sophos Ltd, for who we use their Firewall (Sophos XG) and Intercept X technology, are members of the Internet Watch Foundation (IWF) and block access to illegal Child Abuse Images and Content (CAIC). https://www.iwf.org.uk/membership/our-members/sophos/

The filtering system cannot, however, provide a 100% guarantee that it will do so, because the content on the web change on a daily basis and new technologies are constantly being developed. It is important, therefore, to understand that filtering is only one element in a larger strategy for E-Safety and acceptable use

Internet access is filtered for all users, but these are customised to allow young people more access to certain sites when necessary. Differentiated internet access is available for staff and customised filtering changes are managed by the school. Illegal content is filtered by broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list and other illegal content lists. Filter content lists are updated daily and internet use is logged and frequently monitored. The monitoring process alerts the school to breaches of the filtering policy, which are then acted upon. There is a clear route for reporting and managing changes to the filtering system. Where personal mobile devices are allowed internet access through the school network, filtering will be applied that is consistent with school practice.

- The school has differentiated user level filtering hardware firewall through the use of Sophos XG Threat Management suite.
- There is no option of avoidance of these filters using ant TCAT wired or wireless system.
- Filtering or bypassing of particular web pages can be requested by Teaching staff for educational purposes and reviewed by the ICT provider in conjunction with the school safeguarding lead.
- Filtering services **cannot** be turned off completely by request.
- Any mobile connections connecting to TCAT will fall under the same standards as the main school regarding internet filtering with no exceptions.
- Any filtering issues should be reported immediately to the IT provider.

6.1 Artificial Intelligence

The use of AI in computing platforms is developing at a rapid pace and is an evolving topic. Since the release of Chat GPT in November 2022 there has been an explosion of AI integrations into common platforms such as Microsoft Office 365 and the Google Productivity Suite.

There are essentially two strands to consider in terms of AI in education. Firstly, that of enhanced computing capabilities for both staff and young peoplebrought about by large language models such as Chat GPT and Google Bard. Secondly, misuse of AI in the form of plagiarism should be considered.

TCAT's approach to the use of AI is to embrace the technology available but to discuss ethical use with young people in classes. Modelling safe and correct use of AI in classes (by teachers) is essential to ensure that AI is integrated into curriculum for research purposes only in the most appropriate manner for each subject area.

6.2 Keyword filtering

In May 2016 the Government issued the statutory Guidance for "Keeping children safe in education" within this under "Annex C: Online Safety it expresses the need for

appropriate Filtering and Monitoring. In accordance with the guidance from the UK Safer Internet Centre all TCAT schools and academies incorporate a comprehensive piece of software (provided by Senso Cloud) which audits all devices and users, all usage is tracked from printing to deleting files, login attempts, and computer usage.

Senso Cloud are members of the Internet Watch Foundation (IWF) and block access to illegal Child Abuse Images and Content (CAIC).
https://www.iwf.org.uk/membership/our-members/senso/

Further to this all site users are subject to Senso's keyword search, if a user breaches a keyword search a violation is allocated to that user and information such as time/date, which user and on which device is kept and a screenshot taken of the user's screen automatically and stored in a secure database only available to the E-Safety representatives, the information is stored until the user leaves the TCAT primary school.

The system can deliver "false positives" and not all keywords accurately describe a user's intended searches.

- The Safeguarding lead enforces and defines the search criteria and has a full operating knowledge of the software it uses and functions.
- The TCAT Primary school/ICT Provider ensure Senso is operational on a daily bases and have knowledge of its E-Safety uses.
- Qualified teaching staff may use Senso as classroom intervention tool but cannot see the keyword database entries.

Reports are reviewed often and any false positive information is discounted from any users data collection via Senso.

A Data Risk assessment DPIA for Senso and subsequent data collection software has been generated where this policy is refereed to.

6.3 Passwords

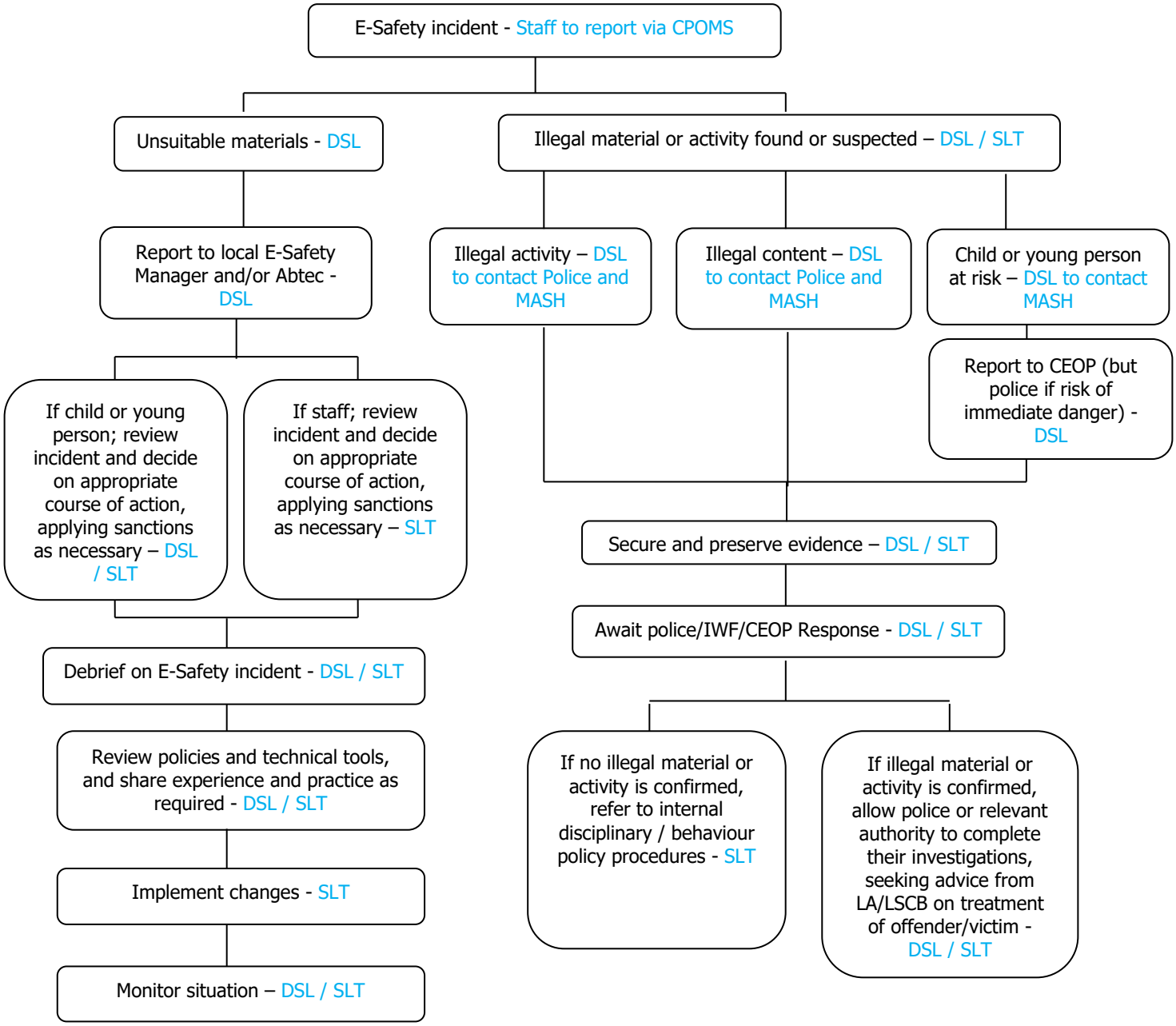
A safe and secure username / password system is essential if the above is to be established and will apply to all school technical systems, including networks, devices and email.

Please refer to this Password & Cyber Security Policy for more information.

- If a user has TCAT approved device such as a laptop we recommend the password to be different than any other password used for other systems

Appendix 1: Responding to Significant Incidents of Misuse

Text in blue refers to who is responsible for acting on the incident at that time.



Glossary of Terms:

- LA – Local Authority
- TCAT – Central TCAT escalation
- MASH – Multi-Agency Safeguarding Hub
- IWF – Internet Watch Foundation
- CEOP – Child Exploitation and Online Protection Centre
- SLT – Senior Leadership Team
- DSL – Designated Safeguarding Lead

7.1 Other Incidents

It is required that a member of the school community will be responsible users of digital technologies within each TCAT Primary school, 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 within this procedure should be followed:

- Have more than one member of child protection staff / involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer(s) 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(s) for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet/Wi-Fi 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, TCAT Primary school current safeguarding software provides this.
- 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 TCAT/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.
  - Extremism or hatred.
  - Radicalism.
  - other criminal conduct, activity or materials.

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 literature should be retained by the group for evidence and reference purposes.

Do not ignore a security incident assuming someone else will report; it is the responsibility of everyone of site to report incidents as soon as they arise.

7.2 School Actions & 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 TCAT Primary school community are aware that incidents have been dealt with. The nature of all of these incidents will vary, in light of this sanctions and actions will be dealt with on an individual case by case basis, in line with the settings Behaviour Policy.

7.3 Training / Awareness of this policy

Members of staff will be made aware of the school's password policy:

- at induction
- Staff Handbook
- through the Acceptable Use Agreement

Young people will be made aware of the school's password policy:

- in lessons
- through the Acceptable Use Agreement

Parents/Community

- On the school's website
- Newsletters

7.4 Audit / Monitoring / Reporting / Review

The responsible person will ensure this policy is up to date:

- Trust Head of IT, yearly review
- Governing Body/Principals – Significant changes present to them
- E-Safety Team/Safeguarding, regular updates review