E-Safety Policy

Approved 13 December 2018
Next Review December 2019

Document control	
Prepared By	DPO
Authorised By	Trustees
Published Location	https://www.dartmoormat.org.uk/policies-and-documents.html

Version control			
Version Number	**Date issued**	**Author**	**Update information**
1.0	13/12/2018	DPO	First Published Version

1. Introduction

1.1. The Dartmoor Multi Academy Trust recognises the role of technology and the internet as part of the statutory curriculum and a necessary tool for learning.

1.2. The safe and appropriate use of technology results from a co-ordinated approach between curriculum leadership, safeguarding leadership, and network management. This policy statement reflects key responsibilities in ensuring this. It forms part of the Trust's protection from legal challenge relating to the use of digital technologies. The Policy should be read in conjunction with other Trust policies including:

1.2.1. Data Protection Policy
1.2.2. Acceptable Use (ICT) Policies for Staff and Pupils
1.2.3. Personal Device (Mobile Phone) Policy
1.2.4. Social Media Policy
1.2.5. CCTV and Surveillance Scheme Policies
1.2.6. Employee Code of Conduct
1.2.7. Safeguarding Policy

1.3. The Trust undertakes to:

- annually review and develop this E-safety policy in line with new legislation, technologies and incidents.
- Ensure regular, documented audit of schools' technical infrastructure
- Promote annual events such as Anti-bullying week and Safer Internet Day (SID)
- Provide Trust and school-wide opportunities to discuss e-safety in detail
- Provide information and awareness to parents/ carers through a variety of sources including newsletters, parents' forums, and signposting.

2. Roles and Responsibilities

2.1. Head teachers / Heads of School:

a. ensure the safety (including e-safety) of all members of the school community
b. ensure adequate CPD is provided to staff around e-safety.
c. follow procedures in the event of a serious e-safety allegation being made concerning a member of staff or pupil within school
d. ensure e-Safety is considered alongside other safeguarding discussions at each staff meeting
e. Monitor e-safety incidents to inform future areas of teaching/learning or training

2.2. School Network Manager

a. Ensure the school's infrastructure is secure and not open to misuse/attack
b. Prepare a network security audit on an annual basis
c. Ensure monitoring is carried out of internet sites used across the school in line with CAIC lists (or ensure that third party monitoring and filtering complies with these requirements)
d. Manage, review and monitor the school filtering policy with school leadership on a regular basis
e. Review breaches with school leadership regularly

2.3. Curriculum leadership

a. Ensure a planned Esafety curriculum is provided, ensuring relevance, breadth and progression, as part of PHSE or other lessons, including sharing relevant resources with teaching teams such as CEOPS.
b. Ensure appropriate training within the school community on Esafety

c. Ensure staff are aware of procedures in the event of an Esafety incident

2.4. Teaching/ Support staff

a. Have up to date awareness of e-safety matters and the Trust's E-safety policy (and associated policies) and practices

b. Embed E-safety issues in all aspects of the curriculum, as well as pastoral/ tutorial activities, to ensure that pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations

c. Report any suspected misuse/problem to the IT staff for investigation, action, or sanction as appropriate

d. Guide pupils to age-appropriate websites, checked as suitable for their use

2.5. Designated Safeguarding Leads and Deputy Safeguarding Officers

Safeguarding leadership should ensure they have relevant CPD in Esafety 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

These are child protection issues, not technical issues, where technology provides additional means for child protection issues to develop.

3. Incidents of misuse

3.1. All members of the school community are expected to be responsible users of digital technologies, who understand and follow school policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

3.2. Incidents of misuse should be investigated. (A template is provided in the appendices). More than one senior member of staff should be involved in this process to protect individuals if accusations are subsequently reported. Investigations should be carried out 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. The same computer should be used for the duration of the procedure. The url of any site containing the alleged misuse should be recorded and the nature of the content causing concern should be described. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed and attached to any incident investigation reports form (except in the case of images of child sexual abuse). Any internal response, disciplinary procedures or referral to local authority agencies or the police will depend on the outcome of any investigation.

3.3. 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

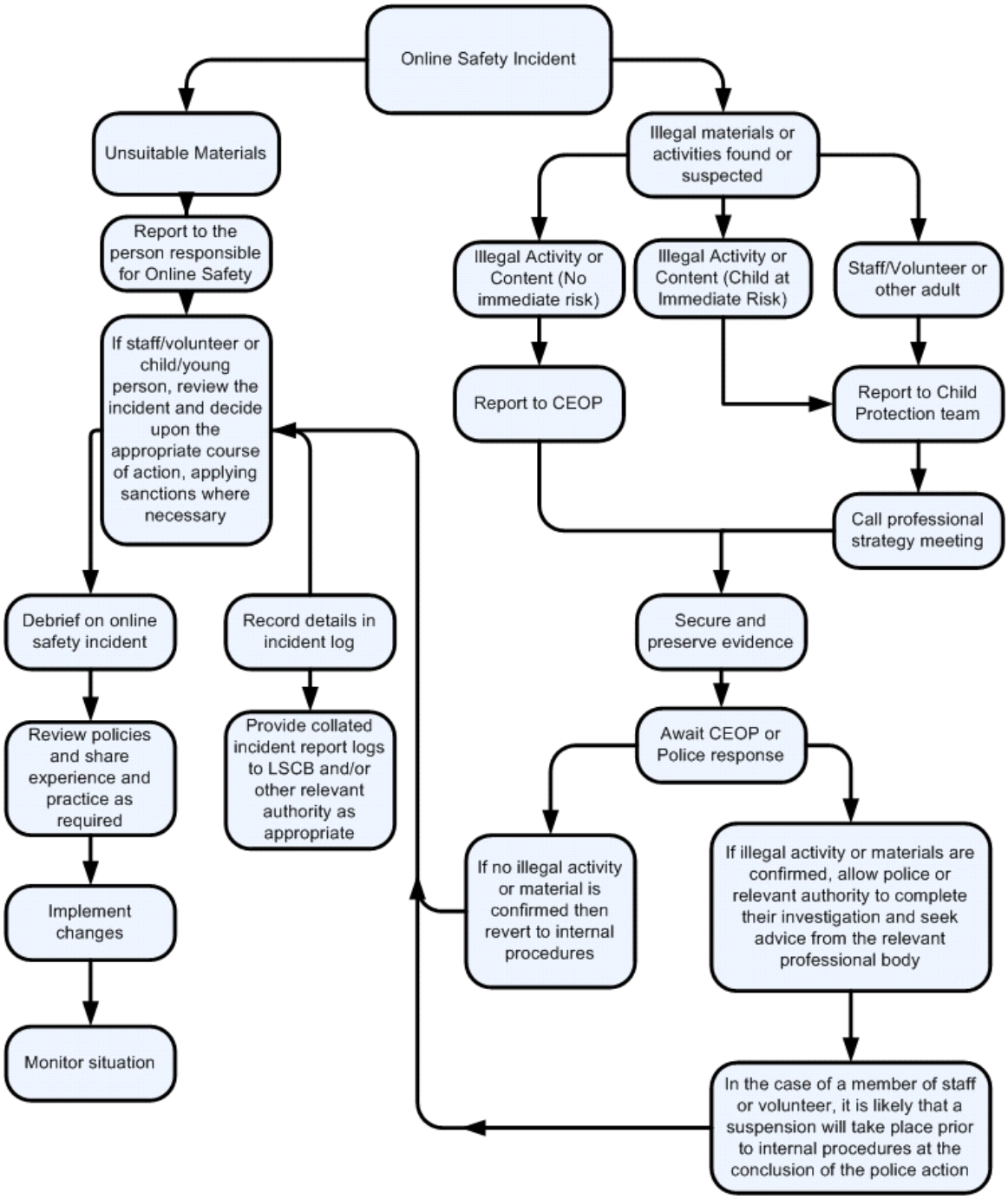
3.4. It is important that all of the above steps are taken as they will provide an evidence trail for the school and possibly the police and demonstrate that visits to these sites were carried out for child protection purposes. Completed documentation should be retained by the school for evidence and reference purposes.

3.5. It is more likely that the schools will need to deal with incidents that involve inappropriate rather than illegal misuse. Incidents of misuse will be dealt with through normal behaviour / disciplinary procedures. All types of misuse cannot be predicted due to the changing nature of ICT. Examples of misuse include:

- Deliberately accessing or trying to access material that could be considered illegal
- Unauthorised use of non-educational sites during lessons
- Accidentally accessing offensive or pornographic material and failing to report the incident
- Deliberately accessing or trying to access offensive or pornographic material
- 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
- Careless use of personal data e.g. holding or transferring data in an insecure manner
- Deliberate actions to breach data protection or network security rules
- Corrupting or destroying data of other users or causing deliberate damage to hardware or software
- Sending an email, text or message regarded as offensive, harassment or of a bullying nature
- Actions which could compromise the staff member's professional standing
- Actions which could bring the school into disrepute or breach the integrity of the school's ethos
- Using proxy sites or other means to subvert the school's filtering system
- Breaching copyright or licensing regulations

3.6. Where the misuse relates to filtering or security breaches, or use of sites which should be filtered, the school's network manager should investigate.

Procedure for responding to Incidents of Misuse



4. ICT Infrastructure, Equipment, Filtering and Monitoring

4.1. Schools within the Dartmoor Multi Academy Trust will be responsible for ensuring that school infrastructure is safe and secure and that procedures within this policy are implemented. The management of technical security will be the responsibility of the school's network manager.

4.2. If the school has a managed ICT service provided by an outside contractor, it is the responsibility of the school to ensure that the managed service provider carries out all the e-safety measures that would otherwise be the responsibility of the school, outlined below. The managed service provider will be made fully aware of the school E-Safety Policy and Acceptable Use Agreements, Data Protection Policies or other relevant policies.

4.3. The school (and service provider) will ensure that:

a. users can only access data to which they have right of access
b. no user should be able to access another's files (other than that allowed for monitoring purposes within the school's policies).
c. access to personal data is securely controlled in line with the school's personal data policy
d. logs are maintained of access by users and of their actions while users of the system
e. there is effective guidance and training for users
f. there are regular reviews and audits of the safety and security of school computer systems
g. there is oversight from senior leaders and these have impact on policy and practice.

4.4. Appropriate security measures are in place through the Antivirus/ Malware protection 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. The school infrastructure and individual workstations are protected by up to date virus software.

4.5. The Network Manager is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations. A record of licences should be maintained.

4.6. All users will have clearly defined access rights to school technical systems. Guests may be granted temporary access onto the school's internet or specific systems by agreement of the school's leadership. Audits should be undertaken annually to ensure appropriate access rights are in place.

4.7. A safe and secure username/password system will apply to all school technical systems, including networks, devices, email.

4.8. Staff will have managed access to DfE approved cloud services (Office 365/ Google Drive) for relevant files.

4.9. Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored. There is a clear process in place to deal with requests for filtering changes.

4.10. The school may monitor and record the activity of users on the school systems.

4.11. Staff who have responsibility for a number of different school systems, including IT staff and Administrators will log these in a secure password protected document.

Appendix 2 Incident Investigation Form

Date	
Reason for investigation	

Details of first reviewing person

Name	
Position	
Signature	

Details of second reviewing person

Name	
Position	
Signature	

Name and location of computer used for review (for web sites)

Reason for concern

Conclusion and Action proposed or taken
