E-Safety Policy

Document control: DMAT E-safety Policy				
Approved by	Trustees		Approved Date	30/04/2020
Published	https://www.dartmoormat.org.uk/policies-and-documents.html		Next Review	30/04/2021
Version	**Date Issued**	**Author**	**Update information**	
1.0	13/12/2018	DPO	First version	
1.1	28/02/2020	N McDermott, J Lake + consultation	Updated. S1.3 added. S2.1 School Leadership definition. S2.2 Hub Network Manager. S2.1f to j added. S4.7 expanded to include DPL duty.	
1.2	30/04/2020	H Fox	1.3 Removal of Online Safety Mark accreditation. Addition of generic Trust investigation form.	

1. Introduction

1.1. The Dartmoor Multi Academy Trust recognises the role of IT 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 reflects key responsibilities in ensuring this and should be read in conjunction with other Trust policies including:

- Data Protection Policy
- Acceptable Use Policies for Staff and Pupils
- Mobile Phone Policy
- Social Media Policy
- CCTV Policy
- Staff Code of Conduct
- Safeguarding Policy
- Child Protection Policy

1.3. The Trust undertakes to:

a. annually review and develop this e-safety policy in line with new legislation, technologies and incidents.
b. Ensure regular, documented audit of schools' technical infrastructure
c. Ensure all schools complete the SWGfL 360 E-safety audit annually and work to support schools to reach the required benchmark levels.

2. Roles and Responsibilities

2.1. School Leadership (Principal/ Executive Head/ Headteacher/ Head 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 including at induction
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
f. Ensuring an annual SWGfL 360 E-Safety audit is completed and shared with the Local Academy Board
g. Ensure all staff complete the Educare Online Safety module annually
h. Promote annual events such as Anti-bullying week and Safer Internet Day (SID)
i. Provide school-wide opportunities to discuss e-safety in detail

j. Provide information and awareness to parents/ carers through a variety of sources including newsletters, parents' forums, and signposting.

2.2. Hub Network Manager

a. Ensure the school's infrastructure is secure and not open to misuse/attack
b. Contribute to the 360 Review with regard to network security
c. Ensure monitoring is carried out of internet sites used across the school in line with Child Abuse Image Content (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 termly
e. Review breaches with school leadership termly.

2.3. Curriculum leadership

a. Ensure a planned E-safety curriculum is provided, ensuring relevance, breadth and progression, as part of PHSE or other lessons, including sharing relevant resources with teaching teams such as Child Exploitation and Online Prevention (CEOP).
b. Ensure appropriate training within the school community on E-safety
c. Ensure staff are aware of procedures in the event of an E-safety 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 School Leadership 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 must ensure they have relevant CPD in E-safety issues and be aware of the potential for serious child protection / safeguarding issues to arise from:

- sharing of personal data
- access to illegal / inappropriate materials
- inappropriate on-line contact with adults / strangers
- potential or actual incidents of grooming
- cyber-bullying

These are child protection issues, not technical issues, where technology provides additional means for child protection issues to develop. The Safeguarding leadership must engage with outside agencies as appropriate e.g. where criminal activity may be suspected.

2.6 Local Academy Boards

a) Monitor the implementation of this policy as part of the overall Safeguarding monitoring at least bi-annually.
b) Monitor the progress and implementation of the action plan from the 360 Review Tool.

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, irresponsible or, very rarely, through deliberate misuse.

3.2. Incidents of misuse will be investigated. A template and flow chart are provided in the appendices. More than one senior member of staff will be involved in this process to protect individuals if accusations are subsequently reported. Investigations must 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 will be used for the duration of the procedure. The url of any site containing the alleged misuse will be recorded and the nature of the content causing concern will 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, the monitoring should be halted and referred to the Police immediately. Other instances to report to the police 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 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 Hub's Network Manager will investigate and report to School Leadership.

4. ICT Infrastructure, Equipment, Filtering and Monitoring

4.1. Schools within the Dartmoor Multi Academy Trust are responsible for ensuring that school infrastructure is safe and secure and that procedures within this policy are implemented. The management of technical security is the responsibility of the Hub Network Manager.

4.2. The school and Hub Manager 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 Trust's Data Protection policy
d. logs are maintained of access by users and of their actions while using the system (e.g. via Smoothwall, inadvertent or deliberate access of unauthorised systems or data)
e. there is effective guidance and training for users
f. there are reviews and audits of the safety and security of school computer systems at least annually
g. there is oversight from senior leaders, and this has impact on policy and practice.

4.3. Appropriate security measures are in place through the Antivirus/ Malware protection to protect the servers, firewalls, routers, wireless systems, workstations, 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.

4.4. The Hub 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.

4.5. All users will have clearly defined access rights to school technical systems**.** Guest temporary access onto the school's internet will be via dedicated Guest profiles. Access to specific school systems will be by agreement of the school's leadership. Audits of network, Office365 / Google Classroom IDs must be undertaken annually by Hub Network Managers to ensure appropriate access rights are in place.

4.6. A safe and secure username/password system will apply to all school technical systems, including networks, devices, email. The School's Data Protection Lead is responsible for ensuring regular audits or registered users for all key systems.

4.7. Internet access is filtered for all users. Illegal content must be filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists must be regularly updated, and internet use must be logged and regularly monitored. Requests for filtering changes must be agreed by the E-Safety Lead or DSL. IT staff must keep a log of such requests (this may be within the filtering system).

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

4.9. Staff who have responsibility for multiple school systems, including IT staff and Administrators, must log user IDs and passwords in a password protected document in Office365/ GSuite to support disaster recovery. Passwords must not be written down.

INVESTIGATION FORM

Investigation Type	☐ *Complaint* ☐ *Incident of Computer Misuse* ☐ *Other* _____
Date first alerted	
Name / Role of Investigator #1	
For Computer Misuse Only Name/ Role of Investigator #2	
Complaint Only Contact details of complainant	
Summary of Issue(s)	
Investigation *Please provide as much detail as possible including evidence collected or not collected, persons interviewed or not interviewed, anonymized statements, third parties, witnesses etc. Please reference any documentary or other evidence.*	
Computer Misuse Only: Name, Serial Number and location of device identified as misused	
Computer Misuse Only: Name, Serial Number and location of device used for review	

Findings	
Recommendations:	
Investigator's signature: **Date:**	
Supporting documents	List all documents collected as part of investigation and included in report
File location	List file path or filing location where documents pertaining to Investigation will be held. Complaints must be held for six years from the date of resolution and then reviewed for further retention in cases of contentious disputes. Retention for cases of Incident Misuse will be as per pupil records then reviewed for further retention in cases of criminal or serious cases.
REVIEW AND SIGN OFF	Name Role Signed Date

Procedure for responding to Incidents of Misuse (Appendix 2)