E-SAFETY POLICY

Document Owner: ICT Network Director
Date: March 2022
Status: Non-statutory

Document Type	E-Safety Policy			
Reference/Version Number	CLT-ESP-V1.3			
Summary	This policy is based on the Department for Education's statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for Academies on preventing and tackling bullying and searching, screening and confiscation. It also refers to the Department's guidance on protecting children from radicalisation.			
Associated Documents	Child Protection and Safeguarding policy Behaviour Policy Social Media Policy Information Technology Policy	Staff Disciplinary Procedures Data Protection Policy and Privacy Notices Complaints Procedure		
Target Audience	All Employees & Students			
Date of this Version	March 2022			
Document Owner	ICT Network Director			
Review Body	Policy Admin Group	**Meeting Date**	17.11.21 16.3.22	
		Meeting Date		
Union Consultation Date/s:	N/A	**Meeting Date**	N/A	
Proof Read	Completed by K Smith 2.3.22			
Senior Leadership Team	N/A			
Approved/Ratified by	Board of Trustees	**Meeting Date**	16.12.19 4.4.22	
Review Frequency	Annual	**Next Review Date**	January 2023	
Signature of Chair of Trustees				

Date uploaded on website/s				
CLT n/r	Haywood n/r	Trentham n/r	Mill Hill n/r	Smallthorne n/r
Date uploaded to Sharepoint/s				
CLT V1.2 - 6.6.22	Haywood V0.1 11.12.20 15:14 V1.2 - 7.6.22	Trentham V0.1 11.12.20 15:14 V1.2 - 7.6.22	Mill Hill V0.1 11.12.20 15:14 V1.2 - 7.6.22	Smallthorne V0.1 11.12.20 15:14 V1.2 - 7.6.22
Acknowledged by Local Governing Committee/s:				
Acknowledged by Local Governing Committee/s:	Haywood 24.3.20 29.3.22	Trentham 25.3.20 30.3.22	Mill Hill 18.3.20 23.3.22	Smallthorne 18.3.20 23.3.22

VERSION CONTROL

Version No:	Type of change	Date	Revisions from previous version
0.1	New Document	Jan 2020	New Policy
1.0	Format	Sept 2020	Corporate format only, no other changes
1.1	Section 4.3	Jan 2021	Generic statement for named Trustee/Governor
1.2	Annual Review	Mar 2022	Information Technology and Social Media policies referenced in Associated Documents and section 14.a
1.3	Interim review from PPWG	Jan 2023	All references to online safety changed to e-safety.

TABLE OF CONTENTS

VERSION CONTROL	2
1. STATUS	4
2. INTRODUCTION	4
3. LEGISLATION & GUIDANCE	4
4. ROLES & RESPONSIBILITIES	4
5. EDUCATING PUPILS ABOUT E-SAFETY	6
6. EDUCATING PARENTS ABOUT E-SAFETY	6
7. CYBER-BULLYING	6
8. ACCEPTABLE USE OF THE INTERNET IN ACADEMY	7
9. PUPILS USING MOBILE DEVICES IN ACADEMY	8
10. STAFF USING WORK DEVICES OUTSIDE ACADEMY	8
11. HOW WILL ACADEMY RESPOND TO ISSUES OF MISUSE	8
12. TRAINING	8
13. MONITORING AND REVIEW	9
14. LINKS WITH OTHER POLICIES	9
APPENDIX A	10
APPENDIX B	11
Acceptable Use Agreement (Staff, Governors, Volunteers and Visitors)	11
APPENDIX C	12

1. STATUS

a. Non statutory.

2. INTRODUCTION

a. Our Academy aims to:
   i. Have robust processes in place to ensure the e-safety of pupils, staff, volunteers and governors
   ii. Deliver an effective approach to e-safety, which empowers us to protect and educate the whole Academy community in its use of technology
   iii. Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

3. LEGISLATION & GUIDANCE

a. This policy is based on the Department for Education's statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for Academies on preventing and tackling bullying and searching, screening and confiscation. It also refers to the Department's guidance on protecting children from radicalisation.

b. It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

c. The policy also takes into account the National Curriculum computing programmes of study.

d. This policy complies with our funding agreement and articles of association.

4. ROLES & RESPONSIBILITIES

4.1 The Governing Committee

a. The Governing Committee in each Academy has overall responsibility for monitoring this policy and holding their respective Headteacher/Principal to account for its implementation.

b. The Governing Committee will co-ordinate regular meetings with appropriate staff to discuss e-safety, and monitor e-safety logs as provided by the Designated Safeguarding Lead (DSL) for each Academy.

c. There is a named Trustee who oversees e-safety within the Trust. There is named Governor in each Academy who oversees e-safety.

d. All Trustees and Governors will:
   i. Ensure that they have read and understand this policy
   ii. Agree and adhere to the terms on acceptable use of the Academy's ICT systems and the internet (Appendix B)

4.2 The Headteacher/Principal

a. The Headteacher/Principal is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the Academy.

4.3 The Designated Safeguarding Lead

a. Details of the Academy's Designated Safeguarding Lead (DSL), Deputy and Safeguarding Officers are set out in our child protection and safeguarding policy.

b. The DSL takes lead responsibility for e-safety in Academy, in particular:

c. Supporting the Headteacher/Principal in ensuring that staff understand this policy and that it is being implemented consistently throughout the Academy

d. Working with the Headteacher/Principal, ICT Network Director and other staff, as necessary, to address any e-safety issues or incidents

e. Ensuring that any e-safety incidents are logged on CPOMS and dealt with appropriately in line with this policy

f. Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the Academy behaviour policy

g. Updating and delivering staff training on e-safety (appendix 3 contains a self-audit for staff on e-safety training needs)

h. Liaising with other agencies and/or external services if necessary

i. Providing regular reports on e-safety in Academy to the Headteacher/Principal and/or Governing Committee

j. This list is not intended to be exhaustive.

4.4 The ICT Network Director

a. The ICT Network Director is responsible for:

   i. Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep pupils safe from potentially harmful and inappropriate content and contact online while at Academy, including terrorist and extremist material

   ii. Ensuring that the Academy's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly

   iii. Conducting regular security checks and monitoring the Academy's ICT systems.

   iv. Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files

   v. Ensuring that any e-safety incidents are logged on CPOMS and dealt with appropriately in line with this policy

   vi. Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the Academy behaviour policy

b. This list is not intended to be exhaustive.

4.5 All Staff and Volunteers

a. All staff, including contractors and agency staff, and volunteers are responsible for:

   i. Maintaining an understanding of this policy. NOTE: The Information Technology and Social Media policies work alongside the E-safety Policy, and should therefore be read in conjunction with this policy.

   ii. Implementing this policy consistently

   iii. Agreeing and adhering to the terms on acceptable use of the Academy's ICT systems and the internet (appendix 2), and ensuring that pupils follow the Academy's terms on acceptable use (appendix 1)

   iv. Working with the DSL to ensure that any e-safety incidents are logged (see appendix 4) and dealt with appropriately in line with this policy

   v. Ensuring that any incidents of cyber-bullying are recorded and dealt with appropriately in line with the Academy behaviour policy

b. This list is not intended to be exhaustive.

4.6 Parents

a. Parents are expected to:

   i. Notify a member of staff or the Headteacher/Principal of any concerns or queries regarding this policy

   ii. Ensure their child has read, understood and agreed to the terms on acceptable use of the Academy's ICT systems and internet (Appendix A)

b. Parents can seek further guidance on keeping children safe online from the following organisations and websites:

   i. What are the issues?, UK Safer Internet Centre: https://www.saferinternet.org.uk/advice-centre/parents-and-carers/what-are-issues

   ii. Hot topics, Childnet International: http://www.childnet.com/parents-and-carers/hot-topics

   iii. Parent factsheet, Childnet International: http://www.childnet.com/ufiles/parents-factsheet-09-17.pdf

4.7 Visitors and Members of the Community

d. Visitors and members of the community who use the Academy's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (appendix 2).

5. EDUCATING PUPILS ABOUT E-SAFETY

a. Pupils will be taught about e-safety as part of the curriculum.

b. Primary Academies insert:

c. In **Key Stage 1**, pupils will be taught to:

   i. Use technology safely and respectfully, keeping personal information private
   ii. Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

d. Pupils in **Key Stage 2** will be taught to:

   i. Use technology safely, respectfully and responsibly
   ii. Recognise acceptable and unacceptable behaviour
   iii. Identify a range of ways to report concerns about content and contact

e. Secondary Academies insert:

f. In **Key Stage 3**, pupils will be taught to:

   i. Understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy
   ii. Recognise inappropriate content, contact and conduct, and know how to report concerns

g. Pupils in **Key Stage 4** will be taught:

   i. To understand how changes in technology affect safety, including new ways to protect their online privacy and identity
   ii. How to report a range of concerns

h. All Academies add:

   i. The safe use of social media and the internet will also be covered in other subjects where relevant.
   ii. The Academy will use assemblies to raise pupils' awareness of the dangers that can be encountered online and may also invite speakers to talk to pupils about this.

6. EDUCATING PARENTS ABOUT E-SAFETY

a. The Academy will raise parents' awareness of internet safety in letters or other communications home, and in information via our website and comms apps. This policy will also be shared with parents.

b. E-safety will also be a topic covered during parents' evenings.

c. If parents have any queries or concerns in relation to e-safety, these should be raised in the first instance with the Headteacher/Principal and/or the DSL.

d. Concerns or queries about this policy can be raised with any member of staff or the Headteacher/ Principal.

7. CYBER-BULLYING

7.1 Definition

a. Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. (See also the Academy behaviour policy.)

7.2 Preventing and Addressing Cyber-Bullying

a. To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

b. The Academy will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Form Tutors/ Teachers will discuss cyber-bullying with their tutor groups, and the issue will be addressed in assemblies.

c. Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

d. All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training (see section 11 for more detail).

e. The Academy also sends information on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected.

f. In relation to a specific incident of cyber-bullying, the Academy will follow the processes set out in the Academy behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the Academy will use all reasonable endeavours to ensure the incident is contained and appropriately dealt with.

g. The DSL will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

7.3 Examining Electronic Devices

a. Academy staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

b. When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

   i. Cause harm, and/or
   ii. Disrupt teaching, and/or
   iii. Break any of the Academy rules

c. If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

   i. Delete that material, or
   ii. Retain it as evidence (of a criminal offence or a breach of Academy discipline), and/or
   iii. Report it to the police

d. Any searching of pupils will be carried out in line with the DfE's latest guidance on screening, searching and confiscation.

e. Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the Academy complaints procedure.

8. ACCEPTABLE USE OF THE INTERNET IN ACADEMY

a. All pupils, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the Academy's ICT systems and the internet (appendices A and B). Visitors will be expected to read and agree to the Academy's terms on acceptable use if relevant.

b. Use of the Academy's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

c. We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

d. More information is set out in the acceptable use agreements in appendices A and B.

9. PUPILS USING MOBILE DEVICES IN ACADEMY

a. Pupils may bring mobile devices into Academy, but are not permitted to use them within the Academy building or during:
    i. Lessons
    ii. Tutor group time
    iii. Clubs before or after Academy, or any other activities organised by the Academy

b. Any use of mobile devices in Academy by pupils must be in line with the acceptable use agreement (see appendix A).

c. Any breach of the acceptable use agreement by a pupil may trigger disciplinary action in line with the Academy behaviour policy, which may result in the confiscation of their device.

10. STAFF USING WORK DEVICES OUTSIDE ACADEMY

a. Staff members using a work device outside Academy must not install any unauthorised software on the device and must not use the device in any way which would violate the Academy's terms of acceptable use, as set out in appendix B.

b. Staff must ensure that their work device is secure and password-protected, and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work device when using it outside Academy. Any USB devices containing data relating to the Academy must be encrypted.

c. If staff have any concerns over the security of their device, they must seek advice from the ICT Network Director.

d. Work devices must be used solely for work activities.

11. HOW WILL ACADEMY RESPOND TO ISSUES OF MISUSE

a. Where a pupil misuses the Academy's ICT systems or internet, we will follow the procedures set out in the behaviour policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

b. Where a staff member misuses the Academy's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

c. The Academy will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

12. TRAINING

a. All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.

b. All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

c. The DSL and safeguarding team will undertake child protection and safeguarding training, which will include e-safety, at least every 2 years. They will also update their knowledge and skills on the subject of e-safety at regular intervals, and at least annually.

d. Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

e. Volunteers will receive appropriate training and updates, if applicable.

f. More information about safeguarding training is set out in our child protection and safeguarding policy.

13. MONITORING AND REVIEW

The DSL monitors behaviour and safeguarding issues related to e-safety through CPOMS.

This policy will be reviewed annually by the Director of Inclusion. At every review, the policy will be shared with the Board of Trustees and the Academy Governing Committee.

14. LINKS WITH OTHER POLICIES

a. This e-safety policy is linked to our:
    i. Child protection and safeguarding policy
    ii. Behaviour policy
    iii. Staff disciplinary procedures
    iv. Data protection policy and privacy notices
    v. Complaints procedure
    vi. Information Technology Policy
    vii. Social Media Policy

APPENDIX A

Acceptable Use Agreement (Pupils and Parents/Carers)

Adapt this agreement to reflect your Academy approach.

Acceptable use of the Academy's ICT systems and internet: agreement for pupils and parents/carers	
Name of pupil:	
When using the Academy's ICT systems and accessing the internet in Academy, I will not: • Use them for a non-educational purpose • Use them without a teacher being present, or without a teacher's permission • Access any inappropriate websites • Access social networking sites (unless my teacher has expressly allowed this as part of a learning activity) • Use chat rooms • Open any attachments in emails, or follow any links in emails, without first checking with a teacher • Use any inappropriate language when communicating online, including in emails • Share my password with others or log in to the Academy's network using someone else's details • Give my personal information (including my name, address or telephone number) to anyone without the permission of my teacher or parent/carer • Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision If I bring a personal mobile phone or other personal electronic device into Academy: • I will not use it during lessons, tutor group time, clubs or other activities organised by the Academy, without a teacher's permission • I will use it responsibly, outside the Academy building and will not access any inappropriate websites or other inappropriate material or use inappropriate language when communicating online I agree that the Academy will monitor the websites I visit. I will immediately let a teacher or other member of staff know if I find any material which might upset, distress or harm me or others. I will always use the Academy's ICT systems and internet responsibly.	
Signed (pupil):	**Date:**
Parent/carer agreement: I agree that my child can use the Academy's ICT systems and internet when appropriately supervised by a member of Academy staff. I agree to the conditions set out above for pupils using the Academy's ICT systems and internet, and for using personal electronic devices in Academy, and will make sure my child understands these.	
Signed (parent/carer):	**Date:**

APPENDIX B

Acceptable Use Agreement (Staff, Governors, Volunteers and Visitors)

Adapt this agreement to reflect your Academy's approach.

Acceptable use of the Academy's ICT systems and the internet: agreement for staff, governors, volunteers and visitors	
Name of staff member/governor/volunteer/visitor:	
When using the Academy's ICT systems and accessing the internet in Academy, or outside Academy on a work device, I will not: • Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature • Use them in any way which could harm the Academy's reputation • Access social networking sites or chat rooms • Use any improper language when communicating online, including in emails or other messaging services • Install any unauthorised software • Share my password with others or log in to the Academy's network using someone else's details	
I will only use the Academy's ICT systems and access the internet in Academy, or outside Academy on a work device, for educational purposes or for the purpose of fulfilling the duties of my role. I agree that the Academy will monitor the websites I visit. I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside Academy, and keep all data securely stored in accordance with this policy and the Academy's data protection policy. I will let the Designated Safeguarding Lead (DSL) and ICT Network Director know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material. I will always use the Academy's ICT systems and internet responsibly, and ensure that pupils in my care do so too. I will use my own personal device whilst out of view of pupils at the Academy.	
Signed (staff member/governor/volunteer/visitor):	**Date:**

APPENDIX C

E-Safety Training Needs – Self-audit for Staff

Adapt this audit form to suit your needs.

E-safety training needs audit	
Name of staff member/volunteer:	**Date:**
Do you know the name of the person who has lead responsibility for E-safety in Academy?	
Do you know what you must do if a pupil approaches you with a concern or issue?	
Are you familiar with the Academy's acceptable use agreement for staff, volunteers, governors and visitors?	
Are you familiar with the Academy's acceptable use agreement for pupils and parents?	
Do you regularly change your password for accessing the Academy's ICT systems?	
Are you familiar with the Academy's approach to tackling cyber-bullying?	
Are there any areas of E-safety in which you would like training/further training? Please record them here.	