Hummersknott Academy Trust

21 – Online Safety Policy

(to be read in conjunction with the Safeguarding Policy and Procedure)

Review Date: July 2021

Adopted/V1	V2	V3	V4	V5	V6		
Oct 2012	July 2014	July 2015	July 2016	July 2017	July 2020		

Hummersknott Academy Trust incorporates Hummersknott Academy and Skerne Park Academy and unless otherwise stated this policy applies to all Academies equally.

PURPOSE

The purpose of this policy is to:

- Give clear guidance to members of the Hummersknott Academy Trust community on safe use of technology and to identify approaches to educate and raise awareness of online safety throughout the community
- Support staff to work safely and responsibly, to role model positive behaviour online and to manage professional standards and practice when using technology

This policy builds upon the Kent County Council/The Education People/Durham County Council online safety policy template, with specialist advice and input as required. This document takes into account the DfE statutory guidance 'Keeping Children Safe in Education' 2019, and Darlington safeguarding procedures.

Hummersknott Academy Trust identifies that the issues classified within online safety are considerable, but can be broadly categorised into three areas of risk:

- **Content:** being exposed to illegal, inappropriate or harmful material
- **Contact:** being subjected to harmful online interaction with other users
- **Conduct:** personal online behaviour that increases the likelihood of, or causes, harm

Many of these risks reflect situations in the off-line world and it is essential that this policy is seen and understood to operate in conjunction with other Academy/Trust policies (e.g. Behaviour Management, Anti-bullying and Safeguarding policies) all of which can be viewed at http://www.hummersknott.org.uk/19/policies-documents or http://www.skernepark.org.uk/documents/

As with all other risks, it is impossible to eliminate them completely. It is therefore essential, through good educational provision, to build student/pupil resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with them.

The Trust recognises that the necessary safeguards must be provided to ensure that everything that could reasonably be expected, in order to manage and reduce these risks, has been implemented. This policy explains how The Trust intends to do this, while addressing wider educational issues in order to help users to be responsible and stay safe whilst online.

SCOPE

This policy applies to all staff, the governing body, leadership team, teachers, support staff, external contractors, visitors, volunteers and other individuals who work for, or provide services on behalf of the the Trust as well as students/pupils, parents and carers (collectively referred to as "staff" in this policy). This policy applies to all access to the internet and use of technology, including personal devices, or where students/ pupils, staff or other individuals have been provided with Trust issued devices for use off-site, such as a work laptops, tablets or mobile phones.

Online safety is an essential part of safeguarding. The Trust acknowledges its duty to ensure that all students/pupils and staff are protected from potential harm online and acknowledges that the internet and associated devices, such as computers, tablets, mobile phones and games consoles, are an important part of everyday life. The Trust believes that students/pupils should be empowered to build resilience and to develop strategies to manage and respond to risk online.

The Education and Inspections Act 2006 empowers Principals/Headteachers, to such extent as is reasonable, to regulate the behaviour of students/pupils when they are off Trust premises and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other online safety incidents covered by this policy, which may take place outside of school, but is

linked to membership of the Trust (see Behaviour Management and Anti-harassment and Bullying Policies for specific information on the jurisdiction of school) http://www.hummersknott.org.uk/19/policies-documents or http://www.skernepark.org.uk/documents/. The Trust will deal with such incidents based on the content of this policy and associated Behaviour Management and Anti-harassment and Bullying Policies and will, where known, inform parents/carers of incidents of inappropriate online safety behaviour.

Links with other policies and procedures

This policy links with several other policies, procedures and action plans

- Behaviour Management Policy
- Safeguarding Policy
- Confidential Reporting (Whistleblowing) Policy
- Curriculum related policies, such as: Personal Social and Health Education (PSHE), Sex and Relationships Education Policy (RSE)
- Data Protection Policy

Monitoring and Review

Technology evolves and changes rapidly. The Trust will review this policy at least annually, it will also be revised following any national or local policy requirements, any child protection concerns or any changes to the technical infrastructure. Internet use will be regularly monitored and online safety mechanisms will be evaluated to ensure this policy is appropriate and fit for purpose.

To ensure they have oversight of online safety, the Designated Safeguarding Lead (DSL) will be informed of online safety concerns, as appropriate. The named governor for safeguarding will report on a regular basis to the governing body on online safety practice and incidents, including outcomes. Any issues identified via monitoring will be incorporated into Academy action planning.

Roles and Responsibilities

The DSL at Hummersknott and Skerne Park Academies have lead responsibility for online safety. ***Whilst activities of the DSL may be delegated to an appropriately trained deputy, overall the ultimate lead responsibility for safeguarding and child protection, including online safety remains with the DSL***.
The Trust recognises that all members of the community have important roles and responsibilities to play with regards to online safety.

The leadership and management team will:

- Ensure that online safety is viewed as a safeguarding issue and that practice is in line with national and local recommendations and requirements
- Ensure there are appropriate and up-to-date policies regarding online safety; including the Staff Code of Conduct and AUP
- Ensure that suitable and appropriate filtering and monitoring systems are in place and work with technical staff to monitor the safety and security of systems and networks.
- Ensure that online safety is embedded within a progressive curriculum, which enables all students/pupils to develop an age-appropriate understanding of online safety
- Support the DSL and any deputies by ensuring they have sufficient time and resources to fulfil their online safety responsibilities
- Ensure there are robust reporting channels for staff to access regarding online safety concerns, including internal, local and national support
- Where appropriate and necessary audit and evaluate online safety practice to identify strengths and areas for improvement

The DSL will:

- Act as a named point of contact on all online safeguarding issues and liaise with other members of staff or other agencies, as appropriate
- Work alongside deputy DSLs to ensure online safety is recognised as part of safeguarding responsibilities and that a coordinated approach is implemented

- Ensure all members of staff receive regular, up-to-date and appropriate online safety training
- Access regular and appropriate training and support to ensure they understand the unique risks associated with online safety and have the relevant knowledge and up to date required to keep students/pupils safe online
- Access regular and appropriate training and support to ensure they recognise the additional risks that students/pupils with Special Educational Needs and Disabilities (SEND) face online
- Keep up-to-date with current research, legislation and trends regarding online safety and communicate this to staff, as appropriate
- Work with staff to coordinate participation in local and national events to promote positive online behaviour, such as Safer Internet Day
- Ensure that online safety is promoted to parents, carers and the wider community, through a variety of channels and approaches
- Maintain records of online safety concerns, as well as actions taken, as part of safeguarding recording mechanisms
- Monitor online safety incidents to identify gaps and trends, and use this data to update the education response, policies and procedures
- Report online safety concerns, as appropriate, to the Principal/Headteacher and Governing Body
- Work with the leadership team to review and update this policy
- Meet regularly with the governor with a lead responsibility for safeguarding and online safety

It is the responsibility of all members of staff to:
- Contribute to the development of the Online Safety Policy
- Read and adhere to the Online Safety and Code of Conduct policies
- Take responsibility for the security of the devices and data they use or have access to
- Model good practice when using technology and maintain a professional level of conduct in their personal use of technology, both on and off site
- Embed online safety education in curriculum deliver, wherever possible
- Have an awareness of a range of online safety issues and how they may be experienced by students/ pupils
- Identify online safety concerns and take appropriate action by following guidance in this policy and related procedure
- Know when and how to escalate online safety issues, including signposting to appropriate support, internally and externally following guidance in this policy and related procedure

It is the responsibility of staff managing the technical environment to:
- Provide technical support and perspective to the DSL and leadership team, especially in the development and implementation of this policy and related procedure
- Implement appropriate security measures as directed by the DSL and leadership team such as the encryption of portable devices and password protection to ensure that the settings IT infrastructure/system is secure and not open to misuse or malicious attack, whilst allowing learning opportunities to be maximised
- Ensure that the firewall capability is assessed on a regular basis
- Ensure appropriate access and technical support is given to the DSL (and/or deputy) to utilise all monitoring and filtering systems to best safeguard users and
- Ensure monitoring systems are fit for purpose and information received is swiftly acted upon

It is the responsibility of students/pupils (at a level that is appropriate to their individual age and ability) to:
- Engage in online safety education opportunities
- Contribute to the development of the Online Safety Policy
- Read and adhere to the AUP
- Respect the feelings and rights of others both on and offline
- Take responsibility for keeping themselves and others safe online
- Seek help from a trusted adult, if there is a concern online, and support others that may be experiencing online safety issues

It is the responsibility of parents and carers to:

- Read the AUP and encourage their children to adhere to it
- Support this policy by discussing online safety issues with their children and reinforcing appropriate and safe online behaviours at home
- Role model safe and appropriate use of technology and social media
- Abide by the AUP
- Identify changes in behaviour that could indicate that their child is at risk of harm online
- Seek help and support from the respective Academy, or other appropriate agencies, if they or their child encounter risk or concerns online
- Contribute to the development of the Online Safety Policy where possible
- Use management systems, learning platforms and other network resources, safely and appropriately
- Take responsibility for their own awareness in relation to the risks and opportunities posed by new and emerging technologies

Community Users

Community users who access Trust ICT systems/websites/VLE as part of the extended provision will be expected **to abide by the AUP. In addition, all users will have to agree to the policy electronically on entry to the Trust ICT network.**

Education and engagement with students/pupils

The Trust will establish and embed a progressive online safety curriculum to raise awareness and promote safe and responsible internet use amongst students/pupils by:

- Ensuring education regarding safe and responsible use, precedes internet access
- Including online safety in PSHE
- RSE and computing programmes of study
- Reinforcing online safety messages whenever technology or the internet is in use
- Educating students/pupils in the effective use of the internet to research; including the skills of knowledge location, retrieval and evaluation
- Teaching students/pupils to be critically aware of the materials they read and shown how to validate information before accepting its accuracy

The Academy will support students/pupils to read and understand the Acceptable User Policy (AUP) in a way which suits their age and ability by:

- Displaying AUP acceptance button on all screens on log-in to Trust systems
- Informing students/pupils that network and internet use will be monitored for safety and security purposes and in accordance with legislation
- Implementing appropriate peer education approaches through the Student Voice/school Council/student leaders
- Providing online safety education and training as part of the transition programme across the key stages and when moving between establishments
- Seeking student/pupil voice when writing and developing the Online Safety Policy, including curriculum development and implementation
- Using support, such as external visitors, where appropriate, to complement and support internal online safety education approaches

Vulnerable Students/Pupils

The Trust recognises that some students/pupils are more vulnerable online due to a range of factors. This may include, but is not limited to children in care, children with SEND or mental health needs, children with English as an additional language and children experiencing trauma or loss. The Trust will ensure that differentiated and ability appropriate online safety education, access and support is provided to vulnerable students/pupils. When implementing the Online Safety Policy and taught online safety curriculum input from specialist staff will be sought as appropriate, including the SENCO, Looked After Children Designated Teacher.

Training and engagement with staff

The Trust will:

- Provide and discuss the Online Safety Policy and Procedure with all members of staff as part of induction
- Provide up-to-date and appropriate online safety training for all staff during annual safeguarding refresher training, and during induction for new staff which will cover the potential risks posed to students/pupils (Content, Contact and Conduct) as well as professional practice expectations
- Recognise the expertise staff build by undertaking safeguarding training and managing safeguarding concerns and provide opportunities for staff to contribute to and shape Online Safety Policy and Procedure.
- Make staff aware that Trust IT systems are monitored, and that activity can be traced to individual users; staff will be reminded to behave professionally and in accordance with the AUP when accessing Trust systems and devices
- Make staff aware that their online conduct outside of work, including personal use of social media, could have an impact on their professional role and reputation
- Highlight useful educational resources and tools which staff should use, according to the age and ability of students/pupils
- Ensure all members of staff are aware of the process to follow regarding online safety concerns affecting students/pupils, colleagues or other members of the community.

Awareness and engagement with parents and carers

Hummersknott Academy Trust recognises that parents and carers have an essential role to play in enabling children and young people to become safe and responsible users of the internet and associated technologies.

The Trust will build a partnership approach to online safety with parents and carers by:

- Providing information and guidance on online safety in a variety of formats
- Drawing their attention to the Online Safety Policy and expectations in newsletters, letters, prospectus and on websites
- Requesting that they read online safety information as part of joining the community, for example, within the home school agreement
- Requiring them to read the AUPand discuss the implications with their children

Responsibility of Each Academy/Trust

- Each Academy is responsible for ensuring that the infrastructure/network is as safe and secure as is reasonably possible
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to Trust ICT systems. Details of the access rights available to groups of users will be recorded by the Network Manager
- All users will be provided with a username and password by a member of Systems Services staff. The Network Manager will keep an up to date record of users and their usernames
- The “master/administrator” passwords for the Trust ICT system, used by the Network Manager, must also be available to the Principal/Headteacher or other nominated senior leader and kept in a secure place (e.g. the school safe)
- The Trust has provided enhanced user-level filtering
- In the event of the Network Manager (or other person) needing to switch off the filtering for any reason, or for any user, this must be logged and carried out by a process that is agreed by the Principal/ Headteacher (or other nominated senior leader)
- Requests from staff for sites to be removed from the filtered list will be considered by a member of Systems Services staff and flagged to the DSL if required
- Trust ICT technical staff regularly monitor and record the activity of users on the Trust ICT systems and users are made aware of this in the AUP
- Remote management tools are used by staff to control students’/pupils’ and visitors’ workstations and view users’ activities

- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, hand held devices, etc. from accidental or malicious attempts which might threaten the security of the Trust systems and data
- The AUP is followed for the provision of temporary access for "guests" (e.g. trainee teachers, visitors) onto the Trust system
- The AUP is followed regarding the extent of personal use that users (staff/students/pupils/community users) and their family members are allowed on laptops and other portable devices that may be used out of school
- The Trust infrastructure and individual workstations are protected by up to date virus software
- Personal data must not be sent over the internet or taken off Academies' sites unless safely encrypted or otherwise secured and with the permission of the E-Safety Co-ordinator

Curriculum

Online Safety is a focus in all areas of the curriculum and staff are expected to reinforce online safety messages in the use of ICT across the curriculum. In lessons where internet use is pre-planned, it is best practice that students/pupils are guided to sites checked as suitable for their use. Where students/pupils are allowed to freely search the internet, e.g. using search engines, staff are expected to be vigilant in monitoring the content of the websites the young people visit.

It is accepted that, from time to time, and for good educational reasons, students/pupils may need to research topics (e.g. racism, drugs, and discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Network Manager temporarily removes those sites from the filtered list for the period of study. Any request to do so must be auditable, with clear reasons for the need. Students/ pupils are taught in all lessons to be critically aware of the materials/content they access online and are guided to validate the accuracy of information, they are also taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.

Students/pupils are explicitly taught how to remain safe whilst accessing the internet. In respect of Hummersknott Academy students, this includes the law surrounding activities such as sexting, file sharing, digital footprint and what can constitute grooming. Skerne Park pupils access a yearly workshop delivered by Durham Constabulary on 'Stranger Danger'. This is aimed at the KS1 pupils; and KS2 sessions focus on keeping safe online and not giving out personal information such as passwords, addresses etc. Skerne Park staff have access to a range of curriculum resources from SWGfL to use in teaching around the topic of online safety.

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students/pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff and students/pupils need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may, as part of a student's/pupil's digital footprint, remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term, indeed, there are many reported incidents of employers carrying out internet searches for information about potential and existing employees. The Trust informs and educates users about the following risks to reduce the likelihood of the potential for harm:-

- When using digital images, staff inform and educate students/pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular students/pupils are taught to recognise the risks attached to publishing their own images on the internet e.g. on social networking sites
- Staff are allowed to take digital/video images to support educational aims
- Such images must only be taken on Trust equipment; equipment owned by staff members must not be used
- Care must be taken when taking digital/video images that students/pupils are appropriately dressed and are not participating in activities that might bring the individuals or the Trust into disrepute
- Students/pupils must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the Academies' websites or elsewhere that include students/pupils will be selected carefully and will comply with good practice guidance on the use of such images

- Permission from parents/carers will be obtained before photographs of students/pupils are published on the Academies' websites
- Student/pupil work can only be published with the permission of the student/pupil and parents/carers

Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:-

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection

Staff must ensure that they:-

- Take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data

Dealing with Breaches of the Policy

Any use that contravenes this policy will be dealt with in line with the Staff Disciplinary Policy and Procedure and may involve withdrawal of ICT usage privileges and potential disciplinary action. These sanctions will be applied at the discretion of the Principal/Headteacher.

This policy links with values 3 – Nothing but the best for all, 4 – Taking responsibility and 8 – Moral Compass of Hummersknott Academy Trust's Vision and Values.

RESPONSIBILITY

This policy will be reviewed and updated where necessary by the Vice Principal of Student Support, Guidance, and Progress and approved for adoption by the Community Committee.

PUBLICISING THE POLICY

A copy of this policy will be available on each Academy's website and the X-drive/intranet where applicable. Staff will be advised of amendments to this policy via the Staff Bulletin/Briefing and are expected to familiarise themselves with the content.

POLICY STATUS

This is a non-statutory policy.

Appendix 1

HUMMERSKNOTT ACADEMY ONLINE SAFETY CURRICULUM MAP

Year	Content
7	**ICT** – Autumn Term: Internet Safety Project using Barclays Digital Safety Resources. **PSHE –** Tutor Programme relating to bullying and online safety, assemblies on anti-bullying and staying safe.
8	**PSHE –** Tutor Programme relating to abuse and Life Skills Days focusing on online grooming, child sexual exploitation and staying safe within the community, assemblies on anti-bullying and staying safe.
9	**ICT – Summer Term:** Cybercrime Project involving staying safe from computer viruses and phishing internet scams. **PSHE** – Taught lessons on types of relationships and consent, Life Skills Day on healthy relationships, assemblies on anti-bullying and staying safe.
10	**ICT -** TLM Digital Skills Course (pending approval) **PSHE** – Taught lessons on Online Safety and grooming (incorporating the 'Trust' film), Tutor Programme relating to body image and the media, and being assertive, Life Skills Day relating to sex and the media (incorporating the dangers of pornography), assemblies on anti-bullying and staying safe.
11	**PSHE –** Taught lessons on abuse and sexting, Tutor Programme relating to healthy relationships, Life Skills Day focusing on online grooming and child sexual exploitation, assemblies on anti-bullying and staying safe.