Hulme Hall Grammar School

E-Safety Policy

Policy Control	
Report	E-Safety Policy
Approval Body	Full Governing Body
Date Reviewed	December 2022
Review Schedule	Annually
Next Review Date	December 2023

Contents

Context

The E-Safety Policy also relates to other documents including the computer use guidance in the employee handbook, Staff Acceptable Use Policy, Pupil ICT Acceptable Use Policy, Anti-Bullying Policy, Behaviour and Discipline Policy and Safeguarding Policy.

Our E-Safety Policy has been written by the School, building on government guidance. It has been agreed by the Senior Leadership Team and approved by Governors.

Roles and Responsibilities

The following policy outlines the online safety roles and responsibilities of all members of the School community (including staff, pupils, volunteers, parents / carers, visitors and community partners).

Teaching and Learning

Why the Internet and Digital Communications are Important

- The internet is an essential element in 21st century life for education, business and social interaction. The School has a duty to provide pupils with quality internet access as part of their learning experience
- Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils
- Internet use will enhance learning
- Internet access has been designed expressly for pupil use and will include filtering appropriate to the age of pupils
- Pupils are taught what internet use is acceptable and what is not and given clear objectives for internet use
- Pupils are educated in the effective use of the internet in research, including the skills of knowledge location, retrieval, and evaluation
- Pupils are shown how to publish and present information to a wider audience
- Pupils are taught how to evaluate internet content
- Internet derived materials used by staff and pupils should comply with copyright law
- Pupils are taught the importance of cross-checking information before accepting its accuracy
- Pupils are taught about online safety
- Pupils are taught to report unpleasant internet content to a member of staff who will share this information with the IT Manager. This information may be passed on to the relevant Key Stage Manager, the Pastoral Manager / DDSL, or the DSL. (The IT Manager can be contacted at ITSupport@hulmehallSchool.org).

Managing Internet Access

Information System Security

- School IT security systems are reviewed regularly by the IT Manager

- Virus protection is updated regularly by the IT Manager.

Email

- Pupils may only use approved email accounts on the School system
- Pupils must immediately tell a teacher if they receive an offensive email
- In email communication, pupils must not reveal their personal details or those of others, or arrange to meet anyone without specific permission
- Incoming email should be treated with care and attachments not opened unless the author is known
- The School does not encourage email from pupils to external bodies unless the contact is well known
- The forwarding of chain letters is not permitted.

Published Content and the School Website

- Staff contact information and pupil details are not available online
- The Headmaster will take overall editorial responsibility and ensure that content is accurate and appropriate. The website will be regularly monitored by the Marketing and Communications Manager.

Publishing Pupil's Images and Work

- Photographs that include pupils will be selected carefully with the permission of parents/guardians
- Pupil's full names will not be used anywhere on a School website or other online space, particularly in association with photographs
- Work can only be published with the permission of the pupil and parents/carers
- Parents are clearly informed of the School policy on image taking and publishing, both on School and independent electronic repositories (see Taking, Storing and Using Images of Children Policy).

Social Networking and Personal Publishing

- The School filters do not allow access to major social networking sites
- Pupils are advised never to give out personal details of any kind which may identify themsleves, their friends, or their location
- Pupils and parents are advised that the use of social network spaces outside School brings a range of dangers for pupils of all ages
- Pupils are advised to use nicknames and avatars when using social networking sites at home.

Managing Filtering

- The School works with their broadband provider to ensure systems to protect pupils are reviewed and improved

- If staff or pupils come across unsuitable online materials, the site must be reported to the IT Manager immediately
- In School, the Governors, SLT and all staff, recognise that School has appropriate filtering and monitoring systems in place and regularly review their effectiveness. The Governors receive IT safety updates from the DSL / leadership team and relevant staff have an awareness and understanding of the provisions in place and manage them effectively and know how to escalate concerns when identified. This is in line with *Keeping Children Safe in Education 2022* and the Prevent duty and the School's Safeguarding policy which is available on the School website.

Managing Videoconferencing and Webcam Use

- Videoconferencing will be carried out using Microsoft Teams, Zoom and School Cloud to ensure quality of service and security, should the School have a need to use this medium
- Pupils will work with a supervising teacher when making or answering a videoconference call in School
- In circumstances where pupils are receiving an education from home, all lessons will be delivered via Microsoft Teams and may be recorded for safeguarding purposes
- Parents will be sent an email informing them of the code of conduct required for online learning (see Student Guide to Using Microsoft Teams).

Managing Emerging Technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in School is allowed
- The Senior Leadership Team should note that technologies such as mobile phones with wireless internet access can bypass School filtering systems and present a new route to undesirable material and communications. Therefore, mobile phones should not be used during lessons or formal School time. In exceptional circumstances, prior permission for such use should be sought by a member of the Senior Leadership Team.
- The sending of abusive or inappropriate text messages or files by Bluetooth or any other means is forbidden
- The use by pupils of mobile phones or cameras in mobile phones will be restricted (see Mobile Phone Policy)
- Care and supervision will be carried out in any use in School or other officially sanctioned location
- The appropriate use of learning platforms will be discussed as the technology becomes available within the School.

Protecting Personal Data

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018.

Authorising Internet Access

- All staff and pupils must read and agree the appropriate "ICT Acceptable Use Policy" before using any School IT resources. This is a signed document by staff, parents and pupils.

- The School will maintain a current record of all staff and pupils who are granted access to School IT systems
- At Year 7, access to the internet will be by adult demonstration, with supervised access to suitable online materials.

Assessing Risks

- The School will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked nature of internet content, it is not possible to guarantee that unsuitable material will never appear on a computer connected to the School network. The School cannot accept liability for any material accessed, or any consequences of internet access
- The School will audit IT use to establish if the E-Safety Policy is adequate and that the implementation of the E-Safety Policy is appropriate and effective.

Handling E-Safety Complaints

- Complaints of internet misuse will be dealt with by a senior member of staff
- Any complaint about staff misuse must be referred to the Headmaster
- Complaints of a child protection nature must be dealt with in accordance with the School's child protection and safeguarding procedures
- Pupils and parents will be informed of consequences for pupils misusing the internet
- Pupils and parents will be informed of the complaints procedure (see the School's Complaints Policy).

Community Use of the Internet

- The School will liaise with local organisations to establish a common approach to E-Safety as the need arises.

Communications Policy

Introducing the E-Safety Policy to Pupils

- E-Safety rules will be posted in all rooms where computers are used and discussed with pupils regularly
- Pupils will be informed that network and internet use will be monitored and appropriately followed up
- A programme of training in E-Safety will be developed, partly based on the materials from the Child Exploitation and Online Protection command (CEOP). E-Safety training will be embedded within the computing scheme of work.

Staff and the E-Safety Policy

- All staff will be given the School E-Safety Policy. It will be available at all times on the School website

- Staff must be informed that network and internet traffic can be monitored and traced to the individual user
- Staff that manage filtering systems or monitor IT use will be supervised by the Senior Leadership Team and work together to resolve issues.

Enlisting Parents' and Carers' Support

- Parents and carers will be made aware of the School E-Safety Policy via the School website
- The School will maintain a list of E-Safety resources for parents/carers to access via the School website or pastoral system
- The School will ask all new parents to sign the Acceptable Use Policy when they register their child with the School.

Safer Practice with Technology

Safer Practice with Technology for Adults Working with Children

The E-Safety Policy and the computer use guidance in the employee handbook responds to questions raised by adults working with children and young people. Adults in this area of work need to ensure they are competent, confident, and safe when working with new technology.

All adults working with children and young people must understand that the nature and responsibilities of their work place them in a position of trust. The E-Safety Policy and the computer use guidance in the employee handbook discuss appropriate and safer behaviour for adults working in paid or unpaid capacities in a School context.

These documents aim to:

- Assist adults to work safely and responsibly and to monitor their own standards and practice
- Help adults to set clear expectations of their own behaviour and to comply with codes of practice
- Minimise the risk of misplaced or malicious allegations being made against adults
- Project a clear message that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary action will be taken
- Support leaders in establishing a culture which safeguards staff and young people.

Hate, Harm and Harassment

General:

There is a range of offences concerned with inciting hatred on the basis of race, religion, sexual orientation etc.

Individual:

There are particular offences to do with harassing or threatening individuals –this includes cyberbullying by mobile phone, social networking sites etc. It is an offence to send indecent, offensive, or threatening messages with the purpose of causing the recipient distress or anxiety.

Inappropriate:

Staff should think about this in respect of professionalism and being a role model. The scope here is enormous but bear in mind that actions outside of the workplace could be so serious as to fundamentally breach the trust and confidence placed in the employee and may constitute gross misconduct.

Headmaster: Mr D Grierson BA, MA (Econ)
Hulme Hall Grammar School, Beech Avenue, Stockport, SK3 8HA
Phone: 0161 485 3524
Email: secretary@hulmehallSchool.org
Hulme Hall Educational Trust (Registered Charity No: 525931)