Hadrian Learning Trust

Online Safety Policy

Online Safety Policy

Contents

Appendices

Online Safety Policy

Aims

Online safety encompasses internet technologies and electronic communications such as mobile phones as well as collaboration tools and personal publishing. It highlights the need to educate pupils/students about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience.

- Our online safety policy relates to other policies including those for ICT, anti-bullying and for child protection
- QEHS has appointed a named person to co-ordinate online safety (Senior Leader responsible for online safety).
- HMS has a named person to co-ordinate online safety (Senior Leader responsible for online safety).
- The online safety policy and its implementation will be reviewed bi-annually unless there is a significant change in provision.

Online safety depends on effective practice at a number of levels:

- Responsible ICT use by all staff and pupils/students.
- Sound implementation of Online safety Policy in both administration and curriculum, including secure school network design and use.
- Safe and secure broadband including the effective management of filtering systems.

Responsibilities

Key responsibilities of students are outlined in the **Student Acceptable Use Agreement** found in Appendix 1. This must be read, understood and signed before access is granted to the school systems.

Key responsibilities of staff are outlined in the **Staff Acceptable Use Agreement** found in Appendix 2. This must be read, understood and signed. In addition, key staff have the following responsibilities:

- The Network Manager and Online Safety Leads will monitor general usage throughout the year
- The designated Online Safety Leads will monitor and act upon "Urgent" and "Critical" alerts daily
- The Business Manager will monitor and act upon the weekly reports
- Safeguarding concerns will be referred to the relevant Designated Safeguarding Lead

Key responsibilities of **parents and carers** are:

- Reading the school's Online Safety Policy and Student Acceptable Use Agreement, encouraging their children to adhere to them, and adhering to them themselves where relevant.
- Discussing online safety issues with their children, supporting the school in their online safety approaches, and reinforcing appropriate safe online behaviours at home.
- Role modelling safe and appropriate uses of new and emerging technologies.
- Identifying changes in behaviour that could indicate that their child is at risk of harm online.
- Seeking help and support from the school, or other appropriate agencies, if they or their child encounters online problems or concerns.
- Taking responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies.

ICT access

- All staff will be signposted to the school Online Safety Policy and have its importance explained. This is part of the induction process.
- All pupils/students are asked to sign (and parents to countersign) a copy of the ICT Acceptable Use Agreement. A copy of the completed agreement is kept in each pupil's/student's individual records file. At QEHS, a copy of the agreement is printed in the student planner.
- The school will keep an up-to-date record of all staff and pupils/students who are granted internet access.
- Pupils/students' access to the internet will be bound by the Student ICT Acceptable Use Agreement.

- Everyone will be made aware that internet traffic can be monitored and can be traced to an individual user.
- Online safety rules will be posted on the school website and internal network and discussed with the pupils/students/staff at the start of each year.
- Staff/pupils/students will be informed that network and internet use will be monitored in accordance with the Staff/Student Acceptable Use Agreements.
- Parents' attention will be drawn to the school's Online Safety Policy in the school's parents' guide and on the school website. Any suitable online safety resources that are produced for parents will be made available.
- The school will take all reasonable precautions to ensure that users access only appropriate 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 school computer. The school cannot accept liability for the material accessed, or any consequences of internet access.

Internet access

- The internet is an essential element for education, business and social interaction. The school has a duty to provide pupils/students 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/students.
- The school internet access is designed for pupil/student use and includes filtering appropriate to the age of pupils/students.
- Pupils/students will be taught what internet use is acceptable and what is not. They will be given clear objectives for internet use.
- The school will ensure that the use of internet derived materials by staff and pupils/students complies with copyright law.
- Information system security, and school ICT systems capacity and security, will be reviewed annually.
- Virus protection will be continuously updated.
- Security strategies will be discussed with relevant staff and appropriate bodies.
- Online safety filtering will be monitored and kept up to date.

Using the internet, social networking and personal publishing

- The school will block/filter access to social networking sites.
- Newsgroups will be blocked unless a specific use is approved.
- Pupils/students will be advised never to give out personal details of any kind which may identify them or their location.
- Pupils/students and parents will be advised on internet safety and of the dangers of the use of social network spaces outside school.
- Pupils/students and parents will be advised that the use of social network spaces outside of school will remain the responsibility of the pupils/students and parents.

Managing filtering

- The school will work with relevant authorities to ensure systems to protect pupils/students are reviewed and improved.
- The Senior Leadership Team will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

Monitoring Internet Use

The school exercises its right to monitor, by electronic means, the use of each school's computer systems, including key logging, the monitoring of web-sites, the interception of e-mails and the deletion of inappropriate materials in circumstances where it believes unauthorised use of the school's computer system is or may be taking place, or the system is or may be being used for criminal purposes or for storing text or imagery which is unauthorised or unlawful. Inappropriate use by students will be addressed through sanctions which may include loss of internet access and/or access to the school network. Inappropriate use by staff will be addressed via the Disciplinary Policy.

Key Logging

The monitoring system sends the Online Safety Lead in each school an alert when the system identifies use that is deemed “critical” or “urgent”. The Online Safety Leads will monitor these alerts and respond appropriately. The Online Safety Leads and Network Manager will monitor general usage throughout the year. In addition, weekly updates are sent to the Business Manager.

Social networking

- Staff and pupils/students will be given regular updates on how to use social media networks responsibly.
- Staff will be made aware that parents and pupils/students may carry out web and social network service searches to find on-line information about staff, for example background, interests, career experiences and self-presentation.

E-mail

- E-communications sent to an external organisation should be written in the same way as a letter written on school headed paper.
- Internal email communications should be professional at all times.
- Incoming email should be treated as suspicious and attachments not opened unless the author is known.

Emerging Technologies and Mobile Phones

- Video-conferencing, where available, will be appropriately supervised for the pupils’/students’ age.
- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- The unauthorised use of cameras of any type is not permitted in school.
- Personal staff mobile phone numbers will not be issued to students or parents. Staff will be issued with a school phone where contact with students is required (e.g. school trip).
- Students can have mobile phones in school provided they are turned off and out of sight during the school day.
- Students can have connected devices in school provided they are turned off and in their bag. Smart watches may be worn provided mobile phones are turned off.
- Where the above rules are not met mobile phones and connected devices will be confiscated and held until the end of the school day (See Screening, Searching and Confiscations Policy).
- Use of mobile phones may be permitted in lessons for educational purposes but only if authorised by teachers, Curriculum Leaders, Pastoral Leaders or the Senior Leadership Team.
- During examinations mobile phones and connected devices that are brought to school must be switched off and handed in. They are not permitted in the exam hall under any circumstances.

Published content and the school web site

- The contact details on the website should be the school address, e-mail and telephone number.
- Pupils’/students’ personal information will not be published.
- Staff personal contact information will not be published. The contact details given online will be the main switchboard and school contact details of selected key personnel only.
- The Executive Headteacher will take overall editorial responsibility and ensure that published content is accurate and appropriate.

Publishing students’/pupils’ images and work

- Photographs that include pupils/students will be selected carefully.
- Pupils/students’ full names will not be used anywhere on the school website particularly in association with photographs without prior permission from parents.

- Written permission from parents or carers will be obtained before photographs of pupils/students are published by the school.
- Pupil/student work can only be published with the permission of the pupil/student and parents/carers.

Protecting personal data

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 or the General Data Protection Regulations.

Reviewed	Date: 14 October 2021

HADRIAN LEARNING TRUST - HEXHAM MIDDLE SCHOOL AND QUEEN ELIZABETH HIGH SCHOOL

STUDENT ICT ACCEPTABLE USE AGREEMENT

Digital technologies have become integral to the lives of children and young people, both within school and outside school. These technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure:

- That young people will be responsible users and stay safe while using the internet and other digital technologies for educational, personal and recreational use.
- That school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.

The school will try to ensure that students will have good access to digital technologies to enhance their learning and will, in return, expect the students to agree to be responsible users.

School Acceptable Use Policy

I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users. It is my responsibility to keep myself and others safe online and be aware of the risks posed by emerging technologies.

For my own personal safety:

- I understand that the school will monitor my use of the systems, devices and digital communications.
- I will keep my username and password safe and secure – I will not share it, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will seek help from a trusted adult if things go wrong, and supporting others who may be experiencing online safety issues.
- I will be aware of "stranger danger", when I am communicating online.
- I will not disclose or share personal information about myself or others when online (this could include names, addresses, email addresses, telephone numbers, age, gender, educational details, financial details etc).
- If I arrange to meet people off-line that I have communicated with online, I will do so in a public place and take an adult with me.
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it online.
- If I discover an unsuitable website, I will report it to a member of staff who will in turn report information to the online safety co-ordinators.

I understand that everyone has equal rights to use technology as a resource and:

- I understand that the school systems and devices are primarily intended for educational use and that I will not use them for personal or recreational use unless I have permission.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not use the school systems or devices for online gaming, online gambling, internet shopping, file sharing, or video broadcasting (e.g. YouTube), unless I have permission of a member of staff to do so.

I will act as I expect others to act toward me:

- I will respect feelings and rights of others both on and offline.
- I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.

- I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will not take or distribute images of anyone without their permission.

I recognise that the school has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the smooth running of the school:

- I will only use my own personal devices (mobile phones / connected devices / USB devices, etc.) in school if I have permission. I understand that, if I do use my own devices in the school, I will follow the rules set out in the Online Safety Policy and this agreement, in the same way as if I was using school equipment.
- I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will not attempt to fix or move equipment or peripherals myself.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I will not open any hyperlinks in emails or any attachments to emails, unless I know and trust the person / organisation who sent the email, or if I have any concerns about the validity of the email
- (due to the risk of the attachment containing viruses or other harmful programmes)
- I will not install or attempt to install or store programmes of any type on any school device, nor will I try to alter computer settings.
- I will not use social media sites when on the school site.

When using the internet for research or recreation, I recognise that:

- I should ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not try to download copies (including music and videos)
- When I am using the internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.

I understand that I am responsible for my actions, both in and out of school:

- I understand that the school also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve my membership of the school community (examples would be cyber-bullying, use of images or personal information).
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I will be subject to disciplinary action. This may include loss of access to the school network / internet, detentions, contact with parents and in the event of illegal activities involvement of the police.

Please complete the sections on the next page to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement, access will not be granted to school systems and devices.

HADRIAN LEARNING TRUST - HEXHAM MIDDLE SCHOOL AND QUEEN ELIZABETH HIGH SCHOOL

STUDENT ICT ACCEPTABLE USE AGREEMENT FORM

This form relates to the Student Acceptable Use Agreement, to which it is attached. Please complete the sections below to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement.

If you do not sign and return this agreement, access will not be granted to school ICT systems.

Declaration

I have read and understand the above and agree to follow these guidelines when:

- I use the school systems and devices (both in and out of school);
- I use my own devices in the school (when allowed) e.g. mobile phones, USB devices etc.;
- I use my own equipment out of the school in a way that is related to me being a member of this school e.g. communicating with other members of the school, VLE, website etc.

Student's Name (please print):		**Year Group**	
Student's Signature:		**Date:**	
Parent's Name (please print):			
Parent's Signature:		**Date:**	

HADRIAN LEARNING TRUST - HEXHAM MIDDLE SCHOOL AND QUEEN ELIZABETH HIGH SCHOOL

STAFF ICT ACCEPTABLE USE AGREEMENT

The school provides network facilities, which includes internet access, to students and staff. This Staff Acceptable Use Agreement will help protect students, staff and the school in general by clearly stating what is acceptable and what is not.

Key responsibilities of staff are:

- Reading the school's Online Safety Policy and Acceptable Use Agreement and adhering to them.
- Contributing to the development of online safety policies.
- Taking responsibility for the security of school systems and data.
- Having an awareness of online safety issues, and how they relate to the children in their care. Knowing when and how to escalate online safety issues, internally and externally.
- Reporting any concerns about specific individuals' online activity and/or safety to the Designated Safeguarding Lead.
- Maintaining a professional level of conduct in their personal use of technology, both on and off site.
- Modelling good practice in using new and emerging technologies and demonstrating an emphasis on positive learning opportunities.
- Not using the school ICT systems for private purposes, unless the Executive Headteacher or Head of School have given permission for that use.
- Not using school systems for personal financial gain, gambling, political purposes or advertising.
- Not using pen drives or external memory to store personal data without suitable encryption or password protection.
- Ensuring that use of the school laptop at home is done responsibly and professionally. Staff should be aware that the majority of websites visited leave evidence on the computer in the form of the history, cookies and images.
- Ensuring that the security of ICT systems is not compromised, whether owned by the school, other organisations or individuals.
- Ensuring that access must only be made via the user's authorised username and password, and that these must not be given to any other person.
- Ensuring that students are not allowed to use staff ICT equipment, as through this, they would have access to confidential information. Any infringements to this would be traced back to the member of staff.
- Ensuring that school computer and internet use is appropriate to education.
- Ensuring that, where personal devices are used to access school content such as emails, staff log out before others use the device.
- Respecting copyright and intellectual property rights.
- Taking steps to ensure that their personal data is not accessible to anybody who does not have permission to access it.
- Taking responsibility for e-mails they send and for contacts made.
- Ensuring that e-mail is written carefully and politely. As messages may be forwarded, email is best regarded as public property.
- Only contacting students, parents or other stakeholders through their work email account.
- Not use mobile phones or connected devices during lesson time or while in charge of children unless doing so to carry out professional responsibilities.
- Not issuing personal mobile phone numbers or email addresses to students or parents.

- Not having online communications with former students who have recently left the school and may have friends or family still within the school.
- Not sending anonymous messages and chain letters.

Use of Social Networking Sites

- The growing popularity of personal web logs (blogs) and social networking sites, such as Facebook and Twitter, may raise issues for the Trust, particularly where employees choose to write about their work in which they are employed.
- Employees must ensure that the content of any blogs/social networking sites do not bring the Trust into disrepute or breach their obligations in relation to confidentiality, professional standards and appropriate behaviour.
- Employees must ensure that privacy and security settings are enabled on their social networking accounts including the prevention of messages being sent to them as a result of an internet search and the control of tags so that they are not tagged in posts that would bring themselves, the school or the Trust into disrepute.
- Employees must not access personal blogs/social networking sites on school equipment or during working hours. When using such sites outside working hours, employees are advised not to write about their work or make reference to the Trust on external web pages. Where an employee chooses to do so, he/she should make it clear that the views expressed are his/hers only and do not reflect the views of the Trust.
- If an employee receives a message on his/her social networking profile that they think could be from a student they must refuse this request and report it to the designated e-safety lead if they believe it may be a cause for concern.
- All employees, including new staff in training and induction, are required to ensure that information available publicly about them is accurate and appropriate.
- Care should be taken not to use language which could be deemed as offensive to others.
- Posting on the schools' official social networking accounts can only be undertaken by those staff who are authorised to do so and in accordance with the online safety policy and acceptable use agreement.

- In addition, employees **must not**:
  - disclose any information that is confidential to the Trust or any third party or disclose personal data of information about any individual/colleague/student/parent/carer which could be in breach of the Trust's (insert name of policy and where available from);
  - disclose any information which is not yet in the public arena;
  - post illegal material, e.g. material which incites racial or religious hatred;
  - link their own blogs/personal web pages to the Trust's website;
  - include any information, sourced from the Trust, which breaches copyright;
  - make any remarks, unless directed to do so by the Trust, about the Trust, colleagues, Trustees/Governors, pupils, parents/carers;
  - publish any material or comment that could undermine public confidence in the individual as an employee of the Trust or in their position within the community;
  - misrepresent the Trust by posting false or inaccurate statements about the work of the Trust;
  - use language which could be deemed as offensive to others;
  - use internet or web-based communication channels to send personal messages to a child/young person, or their parents (including in online gaming);
  - accept former students under the age of 18 as friends as they are still considered minors (the potential for staff to be compromised and open to accusations makes the risk not worth taking);
  - include the name of the school or academy trust in their profile; and/or

- post photographs of students or former students under the age of 18 under any circumstances.

The school may exercise its right by electronic means to monitor the use of the school's computer systems, including the monitoring of web-sites, the interception of e-mails and the deletion of inappropriate materials in circumstances where it believes unauthorised use of the school's computer system is or may be taking place, or the system is or may be being used for criminal purposes or for storing text or imagery which is unauthorised or unlawful. Irresponsible use may result in the loss of internet access and/or access to the school network.

Declaration

I understand and accept the responsibilities contained in the Staff ICT Acceptable Use Agreement. I understand that the school will take all reasonable precautions to ensure students and staff cannot access inappropriate materials. I understand that the school cannot be held responsible for the nature or content of materials accessed through the internet.

Signed: ______________________ Print: ______________________ Date: ______________________