Huddersfield Grammar School

SAFEGUARDING: ONLINE SAFETY POLICY

SEPTEMBER 2016

CONTENTS

1.0 INTRODUCTION

1.1. This policy guidance is designed to guide your practice and policy writing for ensuring strong Online Safety procedures at Huddersfield Grammar School.

1.2 We define Online Safety as:-

- ensuring student Internet use and access is appropriate and controlled.
- preventing misuse of Internet connected devices.
- ensuring students are educated on the risks carried with Internet use and how to minimise and deal with those risks.
- providing students with knowledge and resources to make decisions to ensure their safety online

1.3 Our core principles for Online Safety are:-

- The Internet and Internet connected devices provide a rich resource for supporting teaching and learning.
- We take a whole school, consistent approach to Online Safety, recognising that all staff should be involved and clear on their role in ensuring Online Safety education.
- Online Safety is subject to clear reporting routines and an age appropriate Acceptable Use of Technology Agreement is in place for all students.
- We recognise the need for regular training and ensure at least one member of staff takes accredited training and has a higher level of expertise.
- Our policy reflects current practice and is regularly reviewed and updated by the Lead Team and communicated to all staff.
- Online Safety is addressed within the curriculum at all ages.
- Technology in school is monitored to ensure it offers a safe access point to the Internet
- This policy should complement other school policies, in particular safeguarding policy; staff acceptable Internet and device use; data protection, anti-bullying or similar policies and student / pupil Acceptable Use of Technology Agreement.
- The Online Safety policy is dated with a review date and a named member of staff has

responsibility for ensuring it is reviewed and updated on an annual basis

2.0 WHOLE SCHOOL APPROACH

2.1 We take a consistent approach to Online Safety and ensure that:

- All staff are aware of their responsibilities. Online Safety procedures are discussed in induction for new staff. The policy and procedures are discussed in staff briefings and training is provided at regular intervals.
- Online Safety is mentioned on the SDP noting current state of practice and any areas for development.
- We ensure all students understand what is meant by Online Safety through age appropriate delivery in the curriculum at all ages.
- All pupils are subject to the Acceptable Use of Technology Agreement (AUTA) which is signed by the students and discussed at the start of each new academic year.
- Parents are aware of their children's responsibilities under the AUTA and sign the agreement for younger students/ pupils.
- Awareness raising events are held, such as assemblies, parents' forums and PSCO visits.
- Online Safety is raised as part of school council discussions
- There are notices and posters giving guidance on display in key areas of the school.

3.0 ACCEPTABLE USE OF TECHNOLOGY AGREEMENT AND REPORTING

3.1 We hold an Acceptable Use of Technology Agreement (AUTA) that sets out positive guidelines for how students should use and treat technology both during the school day and outside school as school representatives.
3.2 The AUTA is delivered to all students with a discussion of the points at the beginning of the academic year. The agreement is adapted to the age of the students and older students are expected to sign the agreement. The agreement is presented to students joining the school outside of the start of the academic year.
3.3.The AUTA sets out guidelines for:

- appropriate and respectful use of school technology equipment and devices
- expectations and regulations for the use of students own devices in school
- expectations of behaviour if equipment is found broken or non-functional
- appropriate communications using devices in and out of school
- code of practice if students discover inappropriate or upsetting material on any device
- clear guidance on how to report any concerns

3.4 The AUTA is used positively to encourage appropriate and E-Safe behaviour and can be used alongside rewards for positive use of technology
3.5. The AUTA is supported by a clear set of age appropriate sanctions for behaviour that contradicts the agreement. Sanctions at each level should be recorded and a member of the Lead Team should be made aware of any sanctions applied to students. Records of any behaviour outside the agreement should be held, with clear description of the incident and sanctions applied
3.6 The AUTA is shared with parents and their views are welcomed and considered.
3.7 The AUTA is not intended to form the whole basis of Online Safety education, but to complement discussions and lessons on Online Safety during curriculum time and to provide a robust agreement setting out clear expectations for behaviour
3.8 The AUTA is designed to be binding for students while *enrolled* in the school and the school reserves the right to take action on behaviour that contradicts the Agreement outside of school time. In these cases the school will proceed with discretion and in partnership with parents.

3.9 Students, parents and all staff are able to report concerns and guidance for this should be set out in the AUTA

4.0 STAFF AWARENESS AND TRAINING

4.1 All staff are bound by the code of practice set out in the Cognita Schools Policy for use of Internet and mobile devices. This should be available for all staff and ensures that staff use technology safely and with adherence to safeguarding principles.
4.2 At least one member of staff should undertake accredited training. We recommend the Keeping Children Safe Online (KCSO) course provided by the CEOP. *This training is delivered online and is suggested to take 3 hours in total although it is not necessary for the course to be taken in one 'sitting'.*
4.3 The accredited member of staff should provide a higher level of expertise within the school and can guide staff in Online Safety practice and review of Online Safety policy and procedure and provide INSET guidance
4.4 Online Safety should be built into the termly programme of meetings to ensure all staff are aware of their responsibilities and for the discussion of any issues, concerns or opportunities for events or cross curricular Online Safety lessons.
4.5. There should be a clear procedure for staff wishing to report or discuss concerns relating to Online Safety or Internet access in the school. This procedure should include reporting to a member of Lead Team should be documented as necessary.
4.6 Staff responsibilities for Online Safety are: (for all staff)

- To ensure they are familiar with and fully support the student Acceptable Use of Technology Agreement
- To be vigilant when using technology as part of lessons
- To model safe and responsible use of school technology
- To provide reminders and guidance to students on acceptable use
- To report and act appropriately if they become aware of, or after any student reports, a concern or an incident involving technology use
- To ensure Online Safety is delivered within the curriculum as appropriate to their student age range and subject area
- To contribute to and discuss Online Safety policy and to have their views heard
- To be aware of the school policy for tackling bullying and how this relates to incidents of cyber-bullying
- To be mindful of protecting data and keeping access to digital information secure by adhering to the school password policy and protecting their accounts from student access.
- To use secure portable data options including password protected or encrypted portable memory devices

5.0 ONLINE SAFETY IN THE CURRICULUM

5.1 Online Safety should be embedded into the curriculum at all age ranges. Lessons should be well planned and resourced and there should be a number of opportunities to discuss a range of Online Safety issues.
5.2 Online Safety is expected to be covered within ICT and PSHE lessons but should not be exclusive to these subject areas and discussion of Online Safety should be explored in other subject areas both while using technology and as a topic as appropriate
5.3 Guidance on minimum coverage in each key stage:-
EYFS – safe and responsible use of technology should be modelled; Suggestions relating to ELG could include:
Communication and Language – pupils aware that they are able to communicate with others using devices – appropriate language and key words associated with technology

Physical development – safe and careful handling of technology
Personal, Social and Emotional development – sharing and cooperating while using technology
Understanding of the World – awareness of devices around us and how they are used to keep us safe, provide us with information
EYFS children should be given opportunities to learn collaboratively with devices

Key Stage 1 – Typical KS1 Online Safety coverage should address: Pupils should be made aware of distinction between personal, private and public information. Pupils should be taught appropriate ways to communicate when using devices and how to respond to unpleasant or distressing comments they may encounter online. They should be made aware that people they do not know are strangers including while playing online games and the importance of using 'usernames' and guarding against volunteering information. They should be taught how to respond if they are distressed or uncertain about any material they are exposed to while online or using technology.

Key Stage 2 – Issues outlined above should be addressed with the addition of: Importance of passwords and cyber security. Understanding of how cyberbullying is using technology to be unpleasant and guidance on how to respond constructively and report any thing that concerns them. Understanding of how social networks allow sharing of information and the importance of keeping information about themselves private. Understanding of how data submitted to the Internet including photographs, comments, emails etc. can be potentially accessed, altered and used by anyone. Clearer understanding of distinction between private and public information. Discussion of support networks and methods of reporting anything they are uncertain or concerned about. Understanding of spam, unsolicited and scam activity on the Internet and how accounts can be hacked or accessed by criminals.

Key Stage 3 and 4– Issues outlined above are all relevant with the addition of: Discussion of Online Safety issues in the news and current affairs. Understanding of the law and relevant acts passed to protect people from discrimination, abuse and exposure to indecent content. Discussion of how photographs, information and comments posted online can be accessed by any one and cannot be retracted or removed easily. Fuller understanding of how everyday use of technology can be made more secure through intelligent password use, vigilance and due care when using public technology facilities. Understanding of plagiarism and copyright laws. Addictive nature of devices. Access to relevant support networks and guidance on dealing with cyberbullying, peer pressure and social aspects of device use.

5.4 Extra –curricular activities such as Safer Internet Day opportunities, visits from local PSCO, school assemblies should be explored but these should not represent the majority of Online Safety teaching or discussion in the academic year. They should be used to support lessons embedded in the curriculum.
5.5 Use of mobile devices during lessons is subject to control and risk management. Expectations of appropriate use of mobile devices are set out in the AUTA for students. This includes students are expected not to share digital images or videos of other students taken during lessons for any purpose other than school use.
5.5 Opportunities for peer mentoring or 'buddy' systems can be explored so that older pupils can act as role models for younger children and provide a further method for students to report concerns

6.0 INFRASTRUCTURE AND DATA MANAGEMENT

6.1 The school Internet access is subject to filtering and control and this is updated regularly
6.2 Staff are aware of how to use safe-searching options and are vigilant during lessons involving Internet access
6.3 Where available, screen watching facilities are used and staff are aware of how to utilise

these resources
6.4 Passwords and digital security is in place to protect data and data is managed in accordance with the relevant DP Acts
6.5 Staff are fully aware of how to report a problem or any incidents relating to data security or Internet control
6.6 Professional communications between the school and other organisations or parents take place within clear professional boundaries, are transparent and open to scrutiny and do not share personal information with students

7.0 MONITORING, AUDIT AND POLICY REVIEW

7.1 The Online Safety policy is dated and an annual review date is stated with a named member of staff responsible for ensuring it is reviewed and updated
7.2 It may be necessary for more frequent reviews if a number of incidents are recorded.
7.3 The review procedure should be:

- An audit of effectiveness of current practice
- A review of guidance published by relevant organisations
- Amendments to be shared with all staff

7.4 To audit Online Safety effectiveness of the current policy the following questions should be considered:

- Has recording of Online Safety incidents been effective – are records kept?
- Did the school feel able to respond effectively to any incidents?
- Were incidents resolved to the best of the school's ability?
- Do all students demonstrate an awareness of Online Safety appropriate to their age?
- Have complaints or concerns with the policy been recorded and addressed?
- Have there been significant developments in technology that should be addressed either within the curriculum or as part of staff awareness training?
- Is the policy clear to all staff and seen as appropriate and working?
- Is the current wording of the Acceptable Use of Technology Agreement fit for purpose and reflective of technology use in the school?
- Do all members of the school community know how to report a problem?
- Is Online Safety observed in teaching and present in curriculum planning documents?

APPENDICES
You should append your policy with:

- The Acceptable Use of Technology Agreement for each age group
- Review notes from Online Safety audits
- Any agreements for BYODD and the school device / mobile phone policy
- Agreed sanctions and rewards attached to the AUTA
- Lists of useful organisations and contacts for reporting safeguarding concerns
- School website policy

Incident Reporting form exemplar

Breach of the Acceptable Use of Technology Agreement **Report of Incident Form**	
Date:	
Date(s) of incident(s):	
Staff member completing form:	
Further staff members dealing with incident:	
Name of student(s) involved:	
Parents informed:	
Location of incident:	
Name of IT Team member informed:	
Please give details of the incident:	
Please give details of sanctions applied / action taken	
Is any follow up action required (additional eSafety lessons, invited speakers, referral etc.)?	
Signed: staff member	
Signed ESafety lead:	

Acceptable Use of Technology Agreement (AUTA)

Huddersfield Grammar School

1. To use school technology, digital resources and school digital services I agree to the terms of this Acceptable Use of Technology Agreement.

All students, regardless of age, must have an AUTA signed by them and countersigned by a parent. Use Agreements are becoming accepted as an essential part of internet safety policy and programmes for schools and other organisations, including businesses.

2. I will use school digital services (including email accounts) and technology purely for school related use.

The use of school resources should be restricted to school related matters. School devices should not be used to play games, browse and subscribe to non-academic websites, or communicate socially with people or any other conduct that does not relate directly to school endeavours.

3. I agree to behave responsibly when using technology and I recognise that I represent the school with all of my actions. I know that if I am unsure about anything that I find or receive using technology I can talk to the teachers in school in confidence.

This helps children and young people to take responsibility for their own actions, and seek advice when they are unsure of what to do. It provides an opportunity for the teacher and student to work through an issue and so avoid the student making an unwise decision which could lead to serious consequences. Young children need ongoing guidance to help them become safe and responsible users of ICT.

4. I will follow the AUTA, and will not join in if others are being irresponsible. I understand that even by forwarding, reading or discussing inappropriate materials, I am becoming involved.

Unfortunately, along with many benefits, technology has also provided new ways to carry out anti-social activities. Bullying and harassment by text message, for example, is becoming a major problem. Often children become involved in these acts through peer pressure without thinking of the consequences.

5. If I accidentally come across mean, rude or dangerous material, I will report this to an adult in school, and I know that I should not show any other students.

Because anyone at all can publish material on the internet, it does contain material which is inappropriate and in some cases illegal. The school has taken a number of steps to prevent this material from being accessed. However, there always remains the possibility that a student may inadvertently stumble across something inappropriate. Encouraging students to tell a teacher immediately if they find something which they suspect may be inappropriate encourages critical thinking and helps children to take responsibility for their actions and keep themselves and others safe.

6. I should feel safe when using technology both in school and at home. If I do not feel safe at any time I should report this immediately to a trusted adult.

Our School strives to create a safe and secure learning environment for all members of the school community. Examples of situations involving the use of ICT which might cause a child to feel unsafe could include: contact being made by a stranger through email or text message, the presence of 'scary' images on a computer screen, and/or misconduct by other students. Staff need to be made aware of such situations as soon as they occur to ensure the school can respond immediately.

7. If I am sharing a computer with someone else, I share the responsibility for how it is used. If there is a problem, I will report it.

Students often work together at a single computer. Any misuse of the computer can be traced back to whoever was logged on at the time. It is important that your child takes responsibility for sensible use of the computer at all times, and tells the teacher if there is any concern.

8. I will check before giving anyone information about myself or others when using the internet or a mobile phone – this includes home and email addresses and phone numbers.

This reduces the risk of your child, or other children being contacted by someone who wishes to upset or harm them or use their identity for purposes which might compromise their privacy.

9. I will not be careless, try to damage, or steal any school ICT equipment.

10. I will not try to stop the network or any other equipment from working properly.

11. If I accidentally break something, or I find it broken when I start to use it, I will report this straight away.

12. I will not print anything without the permission of the teacher.

13. I will not try to change screensavers, desktop backgrounds, themes, software or hardware settings.

14. I will not download any files such as music, videos, or programmes without the permission of the teacher, even if they are for school work. If I am unsure, I will talk to the teachers first.

Many files available on the internet are covered by copyright, and although they can be easily downloaded, it may be illegal to do so. Sometimes even innocent-looking files may contain malicious content such as viruses, or spyware. Some files may contain inappropriate or illegal material.

15. I will ask the teacher to check any disk or ICT device (including all disks, memory storage devices, media players, cameras and mobile phones) I bring from home, before I use it with school equipment.

This rule is designed to protect the school's online security and equipment from viruses which can easily be transferred using disks or other storage devices such as USB sticks or memory cards. If your child is using a disk or other device to transfer work between home and school, it should be freshly formatted, or 'blank', before use. This may also stop any of your own personal material from finding

its way onto the school's equipment. Even though every effort is made to keep school equipment virus-free, you should scan your child's disk or device for viruses before they use it again with your home computer.

16. I will not bring software or games from outside school to use on school equipment.

Installing software from home may cause conflicts with the software installed by the school. Our school must also abide by any licensing requirements included within the software. This means that unless the school has purchased a copy, it will not usually be legally entitled to install the software.

17. I will acknowledge where work has come from if I have copied it from somewhere.

The internet has allowed easy access to a huge range of information which can be incorporated into students' work by simply cutting and pasting. Most of this material is copyrighted, and thus involves intellectual property issues. The value to students' learning is questionable if they have not thought through this information themselves.

18. I will not use the internet, mobile phones or any other ICT equipment to be mean, rude, offensive, or to harass any members of the school community like students and staff, at any time while enrolled in the school.

The basic principles of politeness and respect extend to the use of ICT.

You might like to take this opportunity to have a discussion with your child about their general use of ICT whether in or out of school. It helps keep children safe if they understand that many of these rules should be followed regardless of whose ICT equipment they are using, where they are (for example at home, at school, or at a friend's house), or who they are with.

Signed ……Student

Date:

Signed……Parent

Date: