Hope House School
& Vacation Centre

Transforming the lives of children living on the Autistic Spectrum

E-Safety POLICY

Authors:	Phil Baker
Responsible Organisation:	Hope House School
Date issued:	November 2016
Review date:	November 2017

Version 1

Signed:

Hope House School, Barnby Road, Newark, NG24 3NE
This policy has been read and signed on behalf
of the Directors of Hope House School by ______________________________

Version Control Sheet

Version:	**Date of issue:**	**Date of revision:**	**Used by:**
1	November 2016	November 2017	Terri Westmoreland
2	November 2017		
3			
4			
5			
6			

Introduction

Hope House School and Vacation Centre recognises its responsibility to ensure that all reasonable precautions are taken to ensure that both pupils and staff are safe and educated about the risks and threats posed when using the internet and other areas of ICT.

Overview

This policy applies to all members of Hope House School (including staff, pupils, volunteers, parents/carers, visitors, community users) who have access to and are users of school / ICT systems, both in and out of the school. The Education and Inspections Act 2006 empowers Head teachers to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying or other e-safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data (see appendix for template policy). In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy. Hope House School will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate e-safety behaviour that take place out of school.

Internet Use for Hope House Students

SEN students are potentially more vulnerable and more at risk than others when using ICT:

- Those with learning disabilities may make literal interpretations of content which will affect how they respond.
- They may not understand some of the terminology used.
- Those with more complex needs may not always understand the concept of friendship and therefore trust others naively.
- They may not know how to make judgements about what information is safe to share. This can lead to confusion about trusting others on the internet.
- Some students may be vulnerable to being bullied or to extremism/radicalisation through the internet, and they may not be able to recognise this.
- Some students may not appreciate how their own online behaviour may be seen by someone else as bullying.

Teaching and learning

The internet is an essential element in 21st century life for education, business and social interaction. Hope House School recognises it has a duty to provide students with quality internet access as part of their learning experience, regardless of their learning disabilities and attainment levels. It is also part of the statutory computing curriculum and a necessary tool for staff and students. Hope House School ensures that:

- Students are included in this entitlement, although they need a specialist approach to e-learning, as they do in other curriculum areas.
- The school Internet access is designed expressly for student use and includes filtering appropriate to the needs of our students.
- Students are taught what internet use is acceptable and what is not and given clear objectives for Internet use.
- Students are educated in the effective use of the internet.
- Parents are supported by information on the safe use of the internet for their families where applicable.

Students are taught how to evaluate Internet content

- Hope House School ensures that the use of internet-derived materials by staff and students complies with copyright law.
- Students, who are able to, are taught how to report unpleasant internet content to school staff/adults or parents.

Information system security

- School ICT systems, capacity and security are reviewed regularly.
- Virus protection are updated regularly.
- Security strategies are discussed with the Local Authority

E-mail

- Students are not given their own e-mail accounts on the school system, but where appropriate an approved email address for their use is set up for curriculum purposes that is monitored at all times by the class staff.
- In an email communication, students must not reveal their personal details or those of others, or arrange to meet anyone without specific permission.
- E-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.

Published content and the school website

- The contact details on the Hope House School website are the school address, e-mail, telephone number and sometimes photographs. Staff or students' personal information will not be published.
- The Principal takes overall editorial responsibility and ensure that content is accurate and appropriate.

Students' images and work

- Photographs that include students are selected carefully and will not enable individual students to be clearly identified without parental consent.
- Students' full names will not be used anywhere on the website, particularly in association with photographs.
- Written permission from parents or carers for the use of photographs on the website is requested as part of the annual data collection process.

Social networking and personal publishing

- The school will block/filter access to social networking sites for students.
- Students are advised never to give out personal details of any kind which may identify them or their location.
- Students and parents are advised that the use of social network spaces outside school brings a range of dangers for our students.

Managing emerging technologies

- Emerging technologies are examined for educational benefit and risk assessments are 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. Pupils are not allowed the use of their mobile telephones during the hours of 9.00 am to 3.00 pm.

Staff use of personal devices

- Staff are not permitted to use their own mobile phones or devices for contacting students within or outside of the setting in a professional capacity.
- Mobile phones and personally-owned devices are switched off and kept in their personal lockers within the staff room.
- Staff should not use personally-owned devices, such as mobile phones or cameras, to take photos or videos of students and will only use work-provided equipment for this purpose.

- If a member of staff breaches the school policy, then disciplinary action may be taken.

Protecting personal data

- Personal data are recorded, processed, transferred and made available according to the Data Protection Act 1998.

Assessing risks

- Hope House School takes 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. Hope House School cannot accept liability for any material accessed, or any consequences of Internet access.
- Hope House School will audit ICT provision to establish if the e-safety policy is adequate and that its implementation is effective.
- Hope House School will ensure that monitoring software and appropriate procedures are in place to highlight when action needs to be taken by the school.

Handling e-safety complaints

- Any complaint about staff misuse must be referred to the Principal and if the alleged misuse is by the Principal it must be referred to the chair of The Board of Representatives.
- Any staff misuse that suggests a crime has been committed, a student has been harmed or that a member of staff is unsuitable to work with students are reported by the Principal (who is the DSL) to the LADO.
- Students, parents and staff are informed of the complaints procedure.

Introducing the e-safety policy to students

- E-safety rules, in a format appropriate for our students, are available in classrooms and discussed with students as part of their learning, where appropriate.
- Students are informed that network and Internet use is monitored.
- E-safety training is embedded within the Computing teaching and learning documents.
- Pupils have the opportunity to complete the ASDAN Accreditation 'E-Safety' to develop their understanding and awareness.

Social networking

- Staff are made aware that their use of social networking applications has implications for our duty to safeguard students.
- Students and their parents should not be accepted as friends for any reason by staff and any breach of this policy will result in disciplinary action being taken.
- Hope House School employees are not permitted to be 'friends' on social networking sites to ensure that no information can be passed regarding Hope House School over social networks.
- All staff should bear in mind that information they share through social networking applications, even if they are on private spaces, are still subject to copyright, data protection and Freedom of Information legislation, the Safeguarding Vulnerable Groups Act 2006 and other legislation.

Staff and the e-safety policy

- All staff are made aware of the School e-safety policy and its importance explained.
- A copy of the policy is available in the Principal's office.
- Staff are given individual copies of key information regarding the E-Safety policy to keep in their individual folders for personal reference.
- Staff are made aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

Prevent duty

- Hope House School is fully committed to safeguarding and promoting the welfare of all its pupils. Every member of staff recognises that safeguarding against radicalisation and extremism is no different to safeguarding against any other vulnerability in today's society.
- We protect children from the risk of radicalisation, for example by using filters on the internet to make sure they can't access extremist and terrorist material, or by vetting visitors who come into school to work with pupils.
- Our Safeguarding, Prevent, and E-Safety policies set out our beliefs, strategies and procedures to protect vulnerable individuals from being radicalised or exposed to extremist views, by identifying who they are and promptly providing them with support.