# THE HENRY BOX SCHOOL


# E-safety Protocol

**May 2017**

**INTRODUCTION**

At the Henry Box School we use technology and the internet extensively across all areas of the curriculum. This protocol has been written to support on-line safety, or e-safety, by encouraging appropriate and safe conduct to protect the interests of the whole school community.

**DEFINITIONS & REFERENCES**

**E-safety** - the school's ability to protect and educate pupils and staff in their use of technology and to have the appropriate mechanisms to intervene and support any incident where appropriate.

**Users** - staff, governing body, students, volunteers, visitors and any other person working in or on behalf of the school

**Parents** – any adult with a legal responsibility for the child/young person outside the school e.g. parent, guardian, carer.

**School** – any school business or activity conducted on or off the school site, e.g. visits, conferences, school trips etc.

**Whole School Community** - staff, governing body, students, parents, volunteers, visitors and any other person working in or on behalf of the school

This protocol has regard to

- HBS Anti-bullying policy
- HBS Behaviour, Exclusions and Attendance policy
- Education & Inspections Act 2006
- Keeping Children Safe in Education 2016
- Education Act 2011
- Data Protection Act 1998
- www.e-safetysupport.com
- https://nspcc.csod.com

**AIMS AND OBJECTIVES**

The primary purpose of this protocol is:

- to empower the whole school community to stay safe and risk-free and
- to ensure risks are identified and assessed in order to reduce the level of harm

**PROCEDURE**

In order to safeguard staff and students, we will

- teach the effective, considerate and responsible use of the Internet to students through ICT lessons, assemblies and tutor time
- teach students the importance of not sharing detailed private information
- teach students to be critically aware of the sites/materials they access on-line and how content can be manipulated
- require all staff to complete e-safety training online annually
- ensure that the Designated Safeguarding Leads receive regular e-safety updates and relevant training
- inform staff regularly about e-safety developments via briefings and safeguarding training
- have an Acceptable Use Agreement for staff and students
- expect all staff to act as good role models in their use of digital technologies
- expect staff to be vigilant in lessons in monitoring the content of websites that students visit, including those that may expose students to radicalisation
- record any cyberbullying or inappropriate behaviour on-line and respond accordingly
- ensure that the school network is as safe as is reasonably possible

We will also employ the following:

**Internet Filtering** – we use Smoothwall software that prevents access to inappropriate websites. The ICT Support Team is responsible for ensuring that the filtering is appropriate and that any issues are brought to the attention of the Headteacher.

**Email Filtering** – we use Office 365 tools which prevent any infected email being received by the school. Infected is defined as: an email that contains a virus or script (i.e. malware) that could be damaging or destructive to data, e.g. a spam email such as a phishing message.

**Encryption** – All school devices that hold personal data as defined by the Data Protection Act 1998 are encrypted with Sophos Enterprise encryption. All devices that are kept on school property and which may contain personal data are encrypted. Any breach (i.e. loss/theft of device such as laptop or USB keydrive) must be brought to the attention of the Headteacher.

**Passwords** – all staff and students may access a device only with a unique username and password.

**Anti-Virus** – All capable devices have anti-virus software. This software is updated at least weekly for new virus definitions. ICT Support is responsible for ensuring this task is carried out and will report to the Headteacher if there are any concerns. All USB peripherals such as keydrives are scanned for viruses before use.

**AUAs** – Internet use is granted to staff and students upon acceptance of the Acceptable Use Agreement. Our AUAs include fixed and mobile technologies provided by the school as well as technologies owned by students and staff brought onto the school premises.

**Email** – All staff are reminded that emails are subject to Freedom of Information requests, and as such the email service is to be used for professional work-based emails only. Emails of a personal nature are not permitted. Similarly, use of personal email addresses for work purposes is not permitted.

Students are permitted to use the school email system, and will be given their own email address and password.

**Photos and videos** - All parents are given a Copyright release statement at the point of admission and are asked to inform the school if they do <u>not</u> want images to be released.

**Social Networking** - The Henry Box School is fully supportive of social networking as a tool to engage and collaborate with learners and to engage with parents and the wider school community. The following social media services are permitted for use within Henry Box School and have been appropriately risk-assessed. If staff wish to use other social media, permission must first be sought via the Designated Safeguarding Lead who will advise the Headteacher for a decision to be made. Any new service will be risk- assessed before use is permitted.

- Twitter – used by the school as a broadcast service (see below).
- Facebook – used by the school as a broadcast service (see below.

A broadcast service is a one-way communication method in order to share school information with the wider school community. No persons will be “followed” or “friended” on these services and as such no two-way communication will take place.

In addition,

- consent must be obtained before any image or video of any child is uploaded.
- students may be identified using first names only
- where services are “comment enabled”, comments are to be set to “moderated” or “removed”
- all posted data must conform to copyright law. Images, videos and other resources that are not originated by the school are not allowed unless the owner’s permission has been granted or there is a licence which allows for such use

**Notice and take down policy**
If it come to the school's attention that there is a resource which has been inadvertently uploaded, and the school does not have copyright permission to use that resource, it will be removed within one working day.

**Monitoring**
Internet activity may be monitored in order to ensure that as far as possible that users are not exposed to, or actively seeking to access, illegal or inappropriate websites

**Incidents** - Any e-safety incident must be recorded as per the school's safeguarding procedures and brought to the immediate attention of the Designated Safeguarding Lead. The Headteacher is empowered by law to such extent as is reasonable

- to impose disciplinary penalties for inappropriate behaviour out of school but which is linked to membership of the school, e.g. cyberbullying
- to search for, examine and confiscate electronic devices and examine or erase data.

**ROLES AND RESPONSIBILITIES**

**ICT Technical Support Staff**

Technical support staff are responsible for ensuring that:

- the ICT technical infrastructure is secure and reviewed regularly
- anti-virus mechanisms are fit-for-purpose, up to date and applied to all capable devices
- Windows (or other operating systems) updates are regularly monitored and devices updated as appropriate.
- any e-safety technical solutions such as Internet filtering are operating correctly.
- filtering levels are applied appropriately and according to the age of the user
- passwords are applied correctly to all users regardless of age.
- the IT System Administrator password is changed regularly
- users are not permitted to download or install applications onto a school device without prior agreement

**Designated Safeguarding Lead**
The Designated Safeguarding Lead person is a member of the Strategic Leadership Team who has received training in e-safety issues and who is aware of the potential for serious child protection issues arising from inappropriate on-line contact and sharing of personal data and access to inappropriate materials.

**Teaching and non-teaching staff**

Staff will ensure that:

- they are aware of e-safety matters
- they have read and understood the Acceptable Use Agreement

- they monitor the use of digital technologies in lessons and other school activities and that students adhere to the Acceptable Use Agreement
- any e-safety incident or concern is reported to a Student Manager or the Designated Safeguarding Lead
- all digital communications with students and parents are professional and on school systems only

**Students**

The boundaries of use of ICT equipment and services in this school are given in the student Acceptable Use Agreement. Any deviation or misuse of ICT equipment or services will be dealt with in accordance with the Behaviour policy.

e-Safety is embedded into our curriculum; students will be given the appropriate advice and guidance by staff. Similarly all students will be aware how they can report concerns whilst at school or outside of school.

**Parents**

The school will ensure that parents have the skills and knowledge they need to ensure the safety of children outside the school environment. The school will keep parents up to date with new and emerging e-safety tools and advice via its website, including links to support sites such as Childnet and NSPCC.

Parents must also understand the school needs to have rules in place to ensure that their child can be kept safe. As such parents will sign the Acceptable Use Agreement at the point of admission before access is granted to school ICT equipment or services.

Author: Stephen Stewart
Assistant Headteacher

May 2017