Sherburn High School

Headteacher: Mrs M Williams BA (Hons)

Garden Lane, Sherburn In Elmet, Leeds, LS25 6AS
Tel: 01977 682442
Web: www.sherburnhigh.co.uk Email: admin@sherburnhigh.co.uk

Achievement for all

E-Safety Policy

Reviewed

January 2018

(next review date – January 2019)

Policy Statement

For clarity, the e-safety policy uses the following terms unless otherwise stated:

Users - refers to staff, governing body, school volunteers, students and any other person working in or on behalf of the school, including contractors.

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.

Wider school community – students, all staff, governing body, parents visitors, volenteers, lettees etc.

Safeguarding is a serious matter; at Sherburn High School we use technology and the Internet extensively across all areas of the curriculum. Online safeguarding, known as e-safety is an area that is constantly evolving and as such this policy will be reviewed on an annual basis or in response to an e-safety incident, whichever is sooner.

The primary purpose of this policy is twofold:

- To ensure the requirement to empower the whole school community with the knowledge to stay safe and risk free is met.
- To ensure risks are identified, assessed and mitigated (where possible) in order to reduce any foreseeability of harm to the student or liability to the school.

This policy is available for anybody to read on Sherburn High School's website www.sherburnhigh.co.uk/policies; upon review all members of staff will sign as read and understood both the e-safety policy and the Staff Acceptable Use Policy. A copy of this policy and the Acceptable Use Policy will be available on the School website..

Headteacher Name: Maria Williams Signed: M A Williams

Chair of Governors: Carole Middleton Signed:

Review Date: 08.02.2018 **Next Review:** 01.2019

E-Safety

The e-Safety Policy is important at Sherburn High School for a number of reasons, including:

- To ensure there is a clear and consistent approach responding to incidents.
- To ensure that every person responsible for the children is fully aware of his/her responsibilities.
- To set boundaries of use (goalposts) of any school owned IT equipment, or personal IT equipment used in the school, and set the boundaries of services such as social networking (e.g. blogging, Twitter).

E-Safety highlights the need to educate children and young people about the benefits and risks of using new technologies via the internet and electronic communications. It provides safeguards and awareness for users to enable them to control their online activities.

This E-Safety policy operates alongside with other policies such as Behaviour, Data Protection, Anti-Bullying and Acceptable Use Policies.

E-Safety works on effective practice at a number of levels.

1. Responsible ICT use by all staff and students who are encouraged by education and made explicit through published policies.
2. Implementation of the E-Safety policy in both Administration and Curriculum. This includes secure school network design and use.
3. Providing a safe and secure internet connection with effective management of Smoothwall Internet Filtering and Firewall along with Impero Software.
4. National Education Network standards and specifications.

The E-Safety policy is part of the School Development Plan and relates to other policies including those for Bullying and for Child Protection.

- Sherburn High School has written this E-Safety policy, it has been agreed by SLT and approved by the School Governors
- The E-Safety policy and its implementation will be reviewed annually
- The E-Safety Policy was reviewed by: **Pui Ling Ma & Tim Hobson**
- It was approved by the Governors on: **08.02.2018**

Teaching & Learning

Why the internet is important in education

The internet is an essential element in 21st century life for education business and social interaction. Internet use is a part of the statutory curriculum and a necessary tool for staff and students.

Internet use will enhance learning

The school internet access will be designed expressly for pupil use and will include filtering appropriate to the age of students. Students will be taught what internet use is acceptable and what is not and given clear objectives for internet use. Students will be educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation.

Users will be taught how to evaluate internet content

Sherburn High School will ensure that the use of internet derived material by staff and by pupils complies with copyright law. Users, especially students, will be taught to be critically aware of the materials they read and shown how to validate information before accepting is accuracy.

E-Safety Audit

This audit will help help the School Leadership Team (SLT) assess whether the basics of E-Safety are in place.

Does the school have an E-Safety Policy that complies with NYCC guidance?	**Y / ~~N~~**
Date of latest update: **08.02.2018**	
The policy was agreed by Sherburn High School Governors on: **08.02.2018**	
The policy is available for staff at **www.sherburnhigh.co.uk/policies** and internally at **Q:\Policies**	
Parents are able to access this policy at **www.sherburnhigh.co.uk/policies**	
The designated Child Protection contact: **Mrs M Williams**	
The E-Safety Co-Ordinator is: **Mrs M Williams** and **Miss P Ma**	
Has E-Safety training been provided? Staff Students	 **Y / ~~N~~** **Y / ~~N~~**
Is the "Think U Know" training being considered? https://www.thinkuknow.co.uk/teachers/training/	**Y / ~~N~~**
Do all staff sign an Computer and Internet Acceptable Use Policy on appointment before being issued a login?	**Y / ~~N~~**
Do parents agree that their child will comply with the school Acceptable Use Policy	**Y / ~~N~~**
Has the Computer and Internet Acceptable Use Policy been set out for students?	**Y / ~~N~~**
Is the Acceptable Use Policy displayed where students are able to access computers?	**Y / ~~N~~**
Internet access is provided by an approved educational internet service provider and complies with DfES requirements for safe and secure access.	**Y / ~~N~~**
Has an ICT security audit been initiated by SLT, possibly using external expertise.	**Y / ~~N~~**
Staff with responsibility for managing filtering and network access monitoring work within a set of procedures and are adequately supervised by a member of the SLT?	**Y / ~~N~~**

Policy Governance (Roles & Responsibilities)

Governing Body

The governing body is accountable for ensuring that our school has effective policies and procedures in place; as such they will:

- Review this policy at least annually and in response to any e-safety incident to ensure that the policy is up to date, covers all aspects of technology use within the school, to ensure e-safety incidents were appropriately dealt with and ensure the policy was effective in managing those incidents.
- Appoint one governor to have overall responsibility for the governance of e-safety at the school who will:
  - Keep up to date with emerging risks and threats through technology use.
  - Receive regular updates from the Headteacher in regards to training, identified risks and any incidents.
  - The appointed Safegaurding Govenor is Mrs C Middleton

Headteacher

Reporting to the governing body, the Headteacher has overall responsibility for e-safety within our school. The day-to-day management of this will be delegated to a member of staff, the e-Safety Officer (or more than one), as indicated below.

The Headteacher will ensure that:

- E-Safety training throughout the school is planned and up to date and appropriate to the recipient, i.e. students, all staff, senior leadership team and governing body, parents.
- The designated e-Safety Officer(s) has had appropriate CPD in order to undertake the day to day duties.
- All e-safety incidents are dealt with promptly and appropriately.

E-Safety Officer

The day-to-day duty of e-Safety Officer is devolved to Miss P Ma.
The e-Safety Officer will:

- Keep up to date with the latest risks to children whilst using technology; familiarize him/herself with the latest research and available resources for school and home use.
- Review this policy regularly and bring any matters to the attention of the Headteacher.
- Advise the Headteacher, governing body on all e-safety matters.
- Engage with parents and the school community on e-safety matters at school and/or at home.
- Liaise with the local authority, IT technical support and other agencies as required.
- Retain responsibility for the e-safety incident log; ensure staff know what to report and ensure the appropriate audit trail.
- Ensure any technical e-safety measures in school (e.g. Internet filtering software, behaviour management software) are fit for purpose through liaison with the local authority and/or ICT Technical Support.
- Make him/herself aware of any reporting function with technical e-safety measures, i.e. internet filtering reporting function; liaise with the Headteacher and responsible governor to decide on what reports may be appropriate for viewing.

ICT Technical Support Staff

Technical support staff are responsible for ensuring that:

- The IT technical infrastructure is secure; this will include at a minimum:
  - Anti-virus is fit-for-purpose, up to date and applied to all capable devices.
  - Windows 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; that categories of use are discussed and agreed with the e-safety officer and Headteacher.
  - Passwords are applied correctly to all users regardless of age. Passwords for all users will be a minimum of 8 characters and will adhere to password complexity requirements (see Computer and Internet Acceptable use policy)

All Staff

Staff are to ensure that:

- All details within this policy are understood. If anything is not understood it should be brought to the attention of the Headteacher.
- Any e-safety incident is reported to the e-Safety Officer (and an e-Safety Incident report is made), or in his/her absence to the Headteacher. If you are unsure the matter is to be raised with the e-Safety Officer or the Headteacher to make a decision.

- The reporting flowcharts contained within this e-safety policy are fully understood.

All Students

The boundaries of use of ICT equipment and services at Sherburn High School are given in the student Acceptable Use Policy; 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 fully aware how they can report areas of concern whilst at school or outside of school. Students can report any areas of concern on the CEOP website. There is a link on the school's web page.

Parents and Carers

Parents play the most important role in the development of their children; as such the school will ensure that parents have the skills and knowledge they need to ensure the safety of children outside the school environment. Through parents evenings, school newsletters, tweets, email and magazines, the school will keep parents up to date with new and emerging e-safety risks.

Parents must also understand the school needs have to rules in place to ensure that their child can be properly safeguarded. As such, parents will be provided with a "I do not agree to the Acceptable Use Policy" which will need to be returned to the school if they do not agree to the Acceptable Use Policy. Also Parents are able to find this policy along with the Acceptable Use Policy on the School's website.

Safeguarding Committee

Chaired by the Governor responsible for e-Safety, the e-safety Committee is responsible:

- to advise on changes to the e-safety policy.
- to establish the effectiveness (or not) of e-safety training and awareness in the school.
- to recommend further initiatives for e-safety training and awareness at the school.

Established from volunteer students (student leaders), E-Safety Officer(s), responsible Governor(s) and others as required (eg parents), the Safeguarding committee will meet on a termly basis.

Technology

Sherburn High School uses a range of devices including PC's and laptops. In order to safeguard the student and in order to prevent loss of personal data we employ the following assistive technology:

Internet Filtering – we use a Smoothwall UTM (Unified Threat Management) System which provides both filtering and a firewall that prevents unauthorized access to illegal websites. It also prevents access to inappropriate websites; appropriate and inappropriate is determined by the age of the user and will be reviewed in line with this policy or in response to an incident, whichever is sooner. IT Support are responsible for ensuring that the filtering is appropriate and that any issues are brought to the attention of the Headteacher via IT Support / Esafety Officers.

Email Filtering – we use Office 365 configured with DMARC, DKIM and anti-spam security policies that prevents any infected email to be sent from the school or to be received by the school. Infected is defined as: an email that contains a virus or script (i.e. malware, ransomware) via social engineering that could be damaging or destructive to data; spam email such as a phishing message. Students are also hosted on Office365 that is configured as a sub domain of sherburnhigh.co.uk with strict inbound and outbound policies protecting students from bullying, spam, mailware, ransomeware and CEO Fraud.

Encryption – All school devices that hold personal data (as defined by the Data Protection Act 1998) are encrypted. No data is to leave the school on an un-encrypted device; 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 keydrives) is to be brought to the attention of the Headteacher immediately. The Headteacher will liaise with the local authority to ascertain whether a report needs to be made to the Information Commissioner's Office.

Passwords – All staff and students will be unable to access any device without a unique username and password. Staff and student passwords will change every 52 days or if there has been a compromise, whichever is sooner. IT Support will be responsible for ensuring that passwords are changed.

Anti-Virus – All capable devices will have anti-virus software. This software will be updated at least weekly for new virus definitions. IT Support will be responsible for ensuring this task is carried out, and will report to the Headteacher if there are any concerns. All USB peripherals such as USB/Flash drives are scanned for viruses when files are in use.

Safe Use

Internet – Use of the Internet in school is a privilege, not a right. Internet use will be granted to staff upon signing the staff Acceptable Use Policy; Sixth form students are to sign an Acceptable Use Policy. Students in Years 7 – 11 are issued a permission slip which is to be signed and returned to school if parents don't agree to the policies. School ICT Systems capacity and security will be reviewed regularly by the Network Manager. If staff or students discover and unsuitable site, it must be reported to the E-Safety Co-Ordinator or the Network Manager.

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 hosted by Office365 and as such will be given their own email address. The email address will be made up of their Year Of Entry, Firstname, Surname eg.13john.smith@students.sherburnhigh.co.uk. Student email addresses can only send and receive emails to and from email addresses with a @sherburnhigh.co.uk domain and which have been deemed as OK via the Headteacher.

Photos and videos – Digital media such as photos and videos are covered in the schools' Images Policy

Social Networking / Personal Publishing – Sherburn High School will block/filter access to social networking sites such as twitter. Newsgroups will be blocked unless specific use is approved. Students will be advised to never give out personal details of any kind which may identify them or their location and not place personal photos on any social network space when using social networking outside of school. Students should be advised on security and encouraged to set password, deny access to unknown individuals and how to block unwanted communications, they should be encouraged to invite known friends only and deny access to others.
Twitter is permitted for use within Sherburn High School for staff and the site has been appropriately risk assessed.

In addition, the following is to be strictly adhered to:

- Permission slips (via the school photographic policy) must be consulted before any image or video of any child is uploaded.
- There is to be no identification of students using first name and surname; initials to be used when a safe guarding issue arises.
- 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 (i.e. creative commons).

Notice and take down policy – should it come to the schools 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.

Emerging technologies- Emerging technologies will be examined for educational benefit and a risk assessment with be carried out before use in school is allowed. Students will not use mobile phones during lessons or formal schools time. The sending of abusive or inappropriate text messages is forbidden.

Incidents - Any e-safety incident is to be brought to the immediate attention of the e-Safety Officer, or in his/her absence the Headteacher. The e-Safety Officer will assist you in taking the appropriate action to deal with the incident and to fill out an incident log.

Training and Curriculum - It is important that the wider school community is sufficiently empowered with the knowledge to stay as risk free as possible whilst using digital technology; this includes updated awareness of new and emerging issues. As such, Sherburn High School will have an annual programme of training which is suitable to the audience.

E-Safety for students is embedded into the curriculum; whenever ICT is used in the school, staff will ensure that there are positive messages about the safe use of technology and risks as part of the student's learning. This is done through ICT lessons / Form periods and on Safer Internet Day.

As well as the programme of training we will establish further training or lessons as necessary in response to any incidents.

The e-Safety Officer is responsible for recommending a programme of training and awareness for the school year to the Headteacher and responsible Governor for consideration and planning. Should any member of staff feel they have had inadequate or insufficient training generally or in any particular area this must be brought to the attention of the Headteacher for further CPD.

New members of staff are provided with training on an Ad-Hoc basis.