Shaftesbury School

Aspiration Action Achievement

Esafety Policy

March 2016

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.

Safeguarding is a serious matter; at Shaftesbury 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 the Shaftesbury School website; upon review all members of staff will sign as read and understood both the e-safety policy and the Staff Acceptable Use and Internet Policy (Both available as online declarations). A copy of the Students Acceptable Use and Internet Policy is in the students' planner and at the beginning of each school year must be signed by both student and parent. With the signed declaration page in the planner and acceptance of the terms and conditions, students will be permitted access to school technology including the Internet.

Review:

Title of Policy	E Safety Policy
Adopted	March 2016
Cycle	Annual
Policy Prepared By	Mrs S Hunter
Date of Next Review	Autumn 2017
Date:	Signed:

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.

- A governor will 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.

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, (Esafety coordinator/Head of IT/Computing).

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 Coordinator(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 Coordinator

The day-to-day duty of e-Safety coordinator is devolved to *Sarah Hunter*
The e-Safety coordinator 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.
- 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 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 (or other operating system) 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 coordinator and Headteacher.
    - Passwords are applied correctly to all users regardless of age Passwords for staff will be a minimum of 8 characters.

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 Coordinator (and an e-Safety Incident report is made in SIMS), or in his/her absence to the Headteacher. If you are unsure the matter is to be raised with the e-Safety Coordinator 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 in this school are given in the student Acceptable Use and Internet 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.

Parents and Carers

- Parents play the most important role in the development of their children; as such the school will deliver an safety session to new year 7 students. The school will keep parents up to date with new and emerging e-safety risks, and will involve parents in strategies to ensure that students are empowered – these will be available via the school website.

- 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 sign the student Acceptable Use and Internet Policy before any access can be granted to school ICT equipment or services.

Technology

Shaftesbury School uses a range of devices including PC's, laptops, Apple Macs and Ipads. 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 'PAL ALTO' software 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. The ICT/e-Safety co-ordinator and IT Support are responsible for

ensuring that the filtering is appropriate and that any issues are brought to the attention of the Headteacher.

Email Filtering – we use 'Mail Cleaner' software 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) that could be damaging or destructive to data; 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. 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.

Security Policy – Applies to mobile devices. This enables mobile devices force the user to put a passcode on their device and also stops any unauthorized user accessing the system. Username and passwords are required to access email on a mobile device.

Passwords – all staff and students will be unable to access any device without a unique username and password. Staff and student passwords will change on a termly basis or if there has been a compromise, whichever is sooner. The head of IT and IT Support will be responsible for ensuring that passwords are changed.

Anti-Virus – The anti-virus software used in school is called 'ESET'. 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 keydrives (if you allow them) are to be scanned for viruses before 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 this e-safety and the staff Acceptable Use and Internet Policy; Parents and students upon signing in the planner their acceptance of the Acceptable Use and Internet Policy.

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.
Students are permitted to use the school email system, and as such will be given their own email address. The email address will be made up of their year of joining in year 7 and their surname and first three letters of firstname. 12Smithjoh@shaftesburyschool.co.uk

Photos and videos – Digital media such as photos and videos are covered in the schools' Photographic Policy, and is re-iterated here for clarity. All parents must sign a photo/video release slip at the beginning of each academic year; non-return of the permission slip will not be assumed as acceptance.

Radicalisation/Online Safety– All staff ensure that children are safe from terrorist and extremist material when accessing the internet in schools. Shaftesbury School ensures that suitable filtering is in place.

Cyber-bullying is an aggressive, intentional act carried out by a group or individual using electronic forms of contact repeatedly over time against a victim who cannot easily defend himself/herself. By cyber-bullying, we mean bullying by electronic media such as:

- Bullying by texts or messages or calls on mobile phones
- The use of mobile phone cameras to cause distress, fear or humiliation.
- Posting threatening, abusive, defamatory or humiliating material on websites, to include blogs, personal websites, social networking sites
- Using e-mail to message others
- Hijacking/cloning e-mail accounts
- Making threatening, abusive, defamatory or humiliating remarks in chat rooms, to include Facebook, Bebo, Youtube and Ratemyteacher

LEGAL ISSUES Cyber-bullying is generally criminal in character. There are laws that apply to cyberspace.
Shaftesbury School trains its staff to respond effectively to reports of cyber-bullying or harassment and has systems in place to respond to it. Shaftesbury School endeavours to block access to inappropriate web sites, using firewalls, antivirus protection and filtering systems. Where appropriate and responsible, Shaftesbury School audits ICT communications and regularly reviews the security arrangements in place.

Whilst education and guidance remain at the heart of what we do, Shaftesbury School reserves the right to take action against those who take part in cyber-bullying.

- All bullying is damaging but cyber-bullying and harassment can be invasive of privacy at all times. These acts may also be criminal acts.
- Shaftesbury School supports victims and, when necessary, will work with the Police to detect those involved in criminal acts.
- Shaftesbury School will use, as appropriate, the full range of sanctions to correct, punish or remove pupils who bully fellow pupils or harass staff in this way, both in or out of school.
- Shaftesbury School will use its power of confiscation where necessary to prevent pupils from committing crimes or misusing equipment.
- All members of the School community are aware they have a duty to bring to the attention of the Head any example of cyber-bullying or harassment that they know about or suspect.

Continued online safety is delivered through lessons in KS3, assemblies and an Esafety intranet is available for KS4/5 to access.

Social Networking – there are many social networking services available; Shaftesbury 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 Shaftesbury School and have been appropriately risk assessed; should staff wish to use other social media, permission must first be sought via the safety coordinator who will advise the Headteacher for a decision to be made. Any new service will be risk assessed before use is permitted.

- Blogging – used by staff and students in school.
- 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 "friended" on these services and as such no two-way communication will take place.

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; first name only is to be used.
- Where services are "comment enabled", comments are to be set to "moderated".
- 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.

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

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, Shaftesbury School will have access to material informing them of safety issues which is suitable to the audience.

E-Safety for students is embedded into the Digital Literacy curriculum in KS3, through Tutor sessions, assemblies and drop days; 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.

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

The e-Safety coordinator 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.

Acceptable use and Internet Policy

The staff Policy is available as an online secure document on the school intranet page. Staff are to read and accept the policy. This is then recorded and managed by the headteachers PA.

The link to the Staff AUIP is here:

Click here to view staff AUIP

The student's AUIP is available on Page 11/12 of the student planner.

Shaftesbury School

Aspiration Action Achievement

Acceptable Use and Internet Policy – Students

Our Charter of Good Online Behaviour

Note: All Internet and email activity is subject to monitoring

I Promise – to only use the school ICT for schoolwork that the teacher has asked me to do.

I Promise – not to look for or show other people things that may be upsetting.

I Promise – to show respect for the work that other people have done.

I will not – use other people's work or pictures without permission to do so.

I will not – damage the ICT equipment, if I accidentally damage something I will tell my teacher.

I will not – share my password with anybody. If I forget my password I will let my teacher know.

I will not – use other people's usernames or passwords.

I will not – share personal information online with anyone.

I will not – download anything from the Internet unless my teacher has asked me to.

I will – let my teacher know if anybody asks me for personal information.

I will – let my teacher know if anybody says or does anything to me that is hurtful or upsets me.

I will – be respectful to everybody online ; I will treat everybody the way that I want to be treated.

I understand – that some people on the Internet are not who they say they are, and some people can be nasty. I will tell my teacher if I am ever concerned in school, or my parents if I am at home.

I understand – if I break the rules in this charter there will be consequences of my actions and my parents will be told.

Signed (Parent) :

Signed (Student) : **Date :**

Why we Filter the Internet

Introduction

Whilst sometimes seen as one of the more frustrating IT services in schools, Internet filtering is one item in the e-safety toolbox that is of particular importance. When talking about an Internet filter there are two important aspects:

Very broadly speaking

- **Filtering** - this is a pro-active measure to ensure (as much as possible) or prevent users from accessing illegal or inappropriate (by age) websites.
- **Monitoring** - this is a reactive measure and for the most part means searching, browsing or interrogating filter logs (known as the cache) for Internet misuse.

Why do we Filter and Monitor?

Shaftesbury School filters Internet activity for two reasons:

We filter to ensure

- (as much as possible) that children and young people (and to some extent adults) are not exposed to illegal or inappropriate websites. These sites are (or should be) restricted by category dependent on the age of the user. Exposure would include browsing to specifically look for such material, or as a consequence of a search that returns inappropriate results.
- (as much as possible) that the school has mitigated any risk to the children and young people, and thereby reduces any liability to the school by making reasonable endeavours to ensure the safety of those children and young people.

We monitor for assurance

- (as much as possible) that no inappropriate or illegal activity has taken place.
- To add to any evidential trail for disciplinary action if necessary.