Your Gateway to Success
A personalised journey

Shevington High School

E-Safety Policy

DATE ACCEPTED:	**January 2017**
COMMITTEE:	**School Effectiveness**
DATE FOR NEXT REVIEW:	**September 2018**

I
SHEVINGTON HIGH SCHOOL
Headteacher: Mr J Grant
Shevington Lane, Shevington, Wigan, WN6 8AB
Tel: 01257 400990 Fax: 01257 400992
Website: www.shevingtonhigh.org.uk Email: enquiries@shevingtonhigh.org.uk

Shevington High School's Vision

Together we have the highest expectations for all our students, inspiring and enabling them to become amazing and successful individuals. The Shevington Way is one of:

Shevington Standards

At Shevington High School in order to meet the school vision, Students and Adults are expected at all times to work hard to meet our *5 Shevington Standards* which we have set in order to promote respect and dignity for all. Our attitudes, systems and rules are drawn from and support these standards. They are:-

1. We will show respect for each other at all times

2. We will show respect for School property and another person's property at all times

3. We will show respect for ourselves and others by ensuring that our actions do not put at risk the health and safety of ourselves or others

4. We will show respect for ourselves and others by ensuring a high standard of personal appearance and organisation.

5. We will show respect for ourselves and others by supporting a positive climate for learning

Contents

This E-Safety Policy has been developed under guidance from the LGFL, BECTA and Wigan LEA.

Introduction

Information and Communication Technology (ICT) is seen as an essential tool to support teaching and learning, as well as playing an important role in the everyday lives of children, young people and adults. At SHEVINGTON HIGH SCHOOL we have built in these technologies in order to arm our students with the skills they will need for life-long learning and employment.

The world of ICT is a fast moving environment and covers a wide range of resources including; mobile learning, web-based learning and Virtual Learning Environments (VLE) to name a few. Some of the technologies available to young people in/outside of school are:

- Mobile / Smartphone's features include; video, pictures, texts and web access
- Blogs & Wikis based on Web 2.0 technologies
- Online Forums
- Chat Rooms and Social Networking i.e. Facebook, MySpace and Bebo
- Music and Video Broadcasting
- Laptops
- Websites e.g. Youtube
- Podcasting
- Email & Instant Messaging – MSN
- Virtual Learning Platform – Dashboard

While all these technologies are exciting and beneficial to the learner some of the web-based resources are hard to monitor and are not consistently policed. All users including adults need to be aware of the risks associated with the use of Internet technologies.

At SHEVINGTON HIGH SCHOOL we take the matter of e-safety very serious and we teach all our stakeholders in line with Wigan Safeguarding Children E-Safety Policy how to use web-based technologies safely and legally. We teach our students the appropriate behaviours and thinking skills required for safe Internet use that will keep them safe in and beyond the classroom.

This Acceptable Use Policy and other related e-safety AUP's cover both fixed and mobile technologies within school (such as PC's, Laptops, PDA's, Tablets, Webcams, Smartphone's, Voting Systems etc).

Roles and Responsibilities

E-safety is a very important aspect of strategic leadership in school and is therefore the responsibility of the Head and Governors to ensure that the policy and practice of e-safety is embedded and monitored in our school. The named e-safety co-ordinator at SHEVINGTON HIGH SCHOOL is **Mr M. Edey** who is a member of the Senior Middle Leadership Team (SMLT). It is the e-safety co-ordinator's duty to make sure that current issues and guidance through organisations such as CEOP (Child Exploitation and Online Protection), Becta and Childnet are made known to others in school. The Designated Safeguarding Lead, Mrs C Banks has oversight and responsibility of all e-safety safeguarding concerns.

The schools e-safety policy will be made available by the E-safety co-ordinator to all Governors and SLT and any local or national guideline changes will also be noted.

This policy, supported by the school's AUP's for staff, visitors, governors and students, is to protect the interests of the whole school community.

Staff should understand that phone or online communications with pupils can occasionally lead to misunderstandings or even malicious accusations and must take care always to maintain a professional relationship.

E-Safety Development for Staff

- New and current staff receive information on arrival of all the school's acceptable use policies and must sign and complete the relevant form before access is granted.
- All staff are made aware of the procedures that they must adhere to in the safe guarding of children within the context of e-safety and how to deal with any e-safety or misuse of ICT related technologies incident.
- All staff are fully encouraged to embed e-safety activities within their curriculum area. Our staff receive regular Information and training on e-safety issues via twilight sessions and the e-safety Interest Space on the VLN.
- Staff leaving the school will have their associated accounts removed.

Our E-Safety Message

- The school uses Impero, Microsoft TMG and Sophos to monitor and enforce a strict e-safety environment for everyone who accesses a school computer, laptop, offline laptop or mobile device.
- All pupils will receive annually a copy of the e-safety policy and they must return and sign the Internet/Email access form before they are granted access to the Internet.

E-Safety in the Curriculum

- The school has a framework for teaching Internet skills in ICT and as a discrete subject in other areas.
- The school provides opportunities within a range of curriculum areas to teach about e-Safety.
- Educating pupils on the dangers of technologies that maybe encountered outside school is done informally when opportunities arise and as part of the e-Safety curriculum.
- Pupils are aware of the relevant legislation when using the internet such a data protection and intellectual property which may limit what they want to do but also serves to protect them.
- Pupils are taught about copyright and respecting other people's information and images etc through discussion, modelling and activities.
- Pupils are aware of the impact of online bullying and know how to seek help if they are affected by these issues. Pupils are also aware of where to seek advice and help if they experience problems when using the internet and related technologies; i.e. parent/carer, teacher/trusted staff member, or an organisation such as Childline/CEOP report abuse button.
- Pupils are taught to critically evaluate materials and learn effective searching skills through cross curricular teacher models, discussions and via the ICT curriculum.
- E-Safety rules will be posted in all rooms where computers are used.
- All system users will be informed that network and Internet use will be monitored.

Password Security

- When accessing any computer, Internet or email system, students and staff must accept and adhere to the school E-Safety Acceptable Use Policy or if they decline they will be logged off.
- Students are provided with an individual network and virtual learning platform username and password. They are expected to change the default password to an individual password of their choice.
- Staff users are provided with a network, virtual learning platform and an Admin/Sims .net account which also must meet the schools password policy.
- If you think your password has been compromised it is your sole responsibility to contact ICT Support (ext 217) to get it reset. Any computer misuse by others on your account will be logged as you and appropriate action taken, which could involve the police.
- Members of staff are aware of their individual responsibilities to protect the security and confidentiality of the schools networks, MIS systems and Virtual Learning Platforms, including ensuring that passwords are kept safe, not shared and changed periodically. Staff should also make sure that **NO** machines are left unattended while they are logged on, especially when Sims .net is active for registration.
- When logging on or during registration staff are aware that they should not have the screen projected for all to see, this can lead to passwords being compromised as well as data protection issues.

Data Security

Accessing school data is something that the school takes very seriously.

All important data is backed up on a daily basis, but if any files are accidentally deleted then you must notify Mr L Goulding (Strategic ICT Network Manager) as soon as possible

- Staff are aware of their responsibilities when accessing school data. They must not;
    - Take copies of data held on the admin network unless on school commissioned secured pen drives
    - Allow others to view the data
    - Edit data unless authorised to do so
    - Delete data from the admin network unless authorised to do so
    - Use any other USB pen drive other than the encrypted one provided by the school
    - Use school related data containing pupil or staff personal details on their home computers

Managing Internet Access

At Shevington High School we understand that the Internet is a great resource for teaching and learning. Anyone can view information, send messages, discuss ideas and publish material, which is an invaluable resource to education, but we must identify the risks to young and vulnerable people. All schools Internet activity is regularly monitored by both the school and the Local Authority and any inappropriate use will be dealt with.

The School will take 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. Neither the school nor Wigan Council can accept liability for any material accessed, or any consequences of Internet access.

- The school maintains students will have supervised Internet access to planned teaching material/resources via the schools fixed and mobile technologies.
- Staff will plan and preview any websites before use.
- All users must observe copyright at all times and not distribute any school software or data and must not actively download material or software from the Internet.
- Any homework set that requires the students to access the Internet for research should be checked and monitored by the parent. Parents are advised of this and sent regular e-safety flyers.

School Infrastructure and Filtering Policy

- The school's Internet/Email access is controlled using Sophos UTM directly by our Network Manager. The school has in place complaint filtering which includes the Home Office recommended list of keywords. This includes the use of Sophos and Impero which are both members of the Internet Watch Foundation. Sophos UTM includes filtering of website content and communication in 65+ different languages.
- The school also controls monitored Internet access via Microsoft Threat Management Gateway (TMG) and is the responsibility of Mr L Goulding (Strategic ICT Manager) as a result staff will be informed that network and Internet traffic can be monitored and traced to the individual user and to staff laptops.
- The Network Manager uses reports from Impero to identify any violations and forwards this information to Mr M Edey who will then follow up any issues with the DSL and/or pastoral staff.

- The school does not allow staff and pupils to access Internet logs for the safety of all.
- Class control systems are in place, which allows staff to control access to applications and the Internet using IMPERO
- If staff or students discover any inappropriate content they are advised to contact the e-safety co-ordinator Mr M Edey for further action.
- The ICT Network Manager has the responsibility to make sure that all machines in school have up-to-date Anti Virus software.
- All staff that have the ability to use pen drives are responsible for their own Anti Virus protection at home, which must be kept up-to-date, any violation of this can result in the schools network being infected from a Virus leading to a network failure. It is not the school's responsibility nor the Network Manager's to install or maintain virus protection on personal machines. If pupils or staff wish to bring in work on removable media devices other than the encrypted drive provided by the school it must be given to Mr C. Lewis or Mr L. Goulding (ICT Support team) for a safety/virus check before files are copied to the network.

Social Media Safeguards

Facebook safeguards:

- Our Facebook page has several safety features in place.
- A content filtering system (Impero/Sophos) which has a list of banned words, if any words from the list are used the post is automatically blocked as spam.
- Every comment made is also sent to the administrator first before being deleted or published.
- People can like the Shevington page, this simply means to follow news from our page. No contact is made with pupils or the general public.

Twitter safeguards:

- Twitter is slightly more open than Facebook, allowing people to follow our brand simply means they follow our news. People can mention SHS in a post which they would see and we would see. This would not be shown publicly to every follower.
- Conversations again are not held on Twitter and pupils are not followed back.
- If abusive/threatening messages are sent the person can be blocked from both twitter and facebook.
- CL receives notifications for both on phone/email/ipad/macbook.

Managing Emerging Technologies (Web 2.0)

Web 2.0/Social networking sites offer users a great easy to use, creative and mostly free platform to interact with others or the application. However it is important to recognise that there are issues regarding the appropriateness of some content, contact and culture. We encourage our pupils to think carefully both in school and at home about the way that information can be added and removed by all users, including themselves.

- We currently block by default these sites using the latest Web Filtering software and we monitor all Internet and email access using Sophos Web.
- All pupils and Staff are advised to be cautious about information they upload and information given by others. Information given by others may be misleading and not from whom they say they are.
- Pupils are taught not to display images of themselves or others from school and should not display any content that some other individual could use i.e. full name, address, mobile phone number etc. Once an image is placed online it is very difficult to be removed.
- We tell pupils only to use profiles that are private to them and to deny access to unknown individuals.
- Any incidents of bullying must be reported to the school. We keep all identity and information given confidential.
- Staff may only create blogs, wikis or other Web 2.0 spaces in order to communicate with pupils using the schools Virtual Learning Platform or other systems approved by the Headteacher or Governors.
- Pupils should report any online abuse via email to keepsafe@shevingtonhigh.org.uk which will go directly to the Lead Designtaed Safeguaridng Officer, Mrs Banks

Managing Email Communications

The use of Email above any other method of communication is such an advantage in this hi-tech modern world, and there's no doubt that staff and pupils will have to use it at some point in their lives. Within school email should not be considered private as all email communications to and from school are monitored for various violation of school policy.

Email without doubt offers significant benefits to staff and pupils especially when working on school based projects. In order to meet ICT levels in school, pupils must have experienced sending and receiving emails.

- All staff and pupils in school are given their own unique email address for school business only, this gives us the ability to audit emails in a secure manner.
- It is the responsibility of each email account holder to keep their password secure. For the safety of all users email communications are filtered by Sophos Pure Message and logged and reports are done on a regular basis.
- Staff should not contact pupils or parents or conduct any school business using a personal email address.
- Pupils should only use email for educational purposes under supervision from a teacher.
- Any abuse of the email system/policy witnessed by staff or pupils should be reported to **Mr M. Edey** and the Strategic ICT Manager.
- All email users must adhere to the schools e-safety policy and are reminded that they have accepted both a computer AUP and an Internet/Email policy signed by their parents. The use of explicit language and content is strictly prohibited and any violations of this rule will be severely dealt with.
- Pupils are introduced to email as part of their ICT scheme of work but is not accessible in school other than to e mail staff.
- Pupils must not reveal their personal details or those of others or arrange to meet anyone without specific permission from the Headteacher.

To access the schools email system go to: *https://login.microsoftonline.com/*

Mobile Technologies

Many emerging technologies offer new opportunities for teaching and learning including a move towards personalised learning and 1:1 device ownership for children and young people. Many existing mobile technologies such as PDAs, portable media players, gaming devices, mobile and smart phones are familiar to children outside of school too. They often provide a collaborative, well-known device with possible internet access and thus can open up risk and misuse associated with communication and internet use. All emerging technologies that the school intends to use will be thoroughly examined and tested before implementation in the classroom. We choose to manage the use of the devices in the following ways so that users exploit them appropriately.

- The school allows staff to bring in personal mobile phones and devices for their own use. Under no circumstances does the school allow a member of staff to contact a pupil or parent/carer using their personal device.
- Pupils are allowed to bring in mobile phones. If a pupil is found using them for personal reasons during lessons they will be confiscated.
- The sending of inappropriate text, image and video messages between any member of the school community is not allowed.
- Under no circumstance must content created on the mobile device be uploaded to any web site that shares information i.e. Facebook, MySpace or YouTube that contains any member of the school community. The only exception is to the schools Virtual Learning Network (VLN) with permission.

Safe Use of Images

Please see school policy on photographs and filmed images

Publishing pupil's images and work

All parents and guardians are asked for permission to use their child's work/photos in the following ways:

- On the schools website
- On the schools Virtual learning platform
- In the school prospectus and other printed publications that the school may produce for promotional purposes
- Recorded/transmitted on a DVD, video or webcam
- Broadcast on the schools internal multimedia displays
- In display material that may be used in external areas i.e. art exhibitions etc
- General media appearances i.e. local, national media or press releases sent to the press highlighting an activity

This consent form is considered a valid document for the entire duration of the pupils education at SHEVINGTON HIGH SCHOOL. Pupil names, email, postal address and mobile numbers will not be published against any image.

Storage of Images

- Images of children and staff are stored securely on the schools network.
- Pupils and staff are not permitted to use personal portable media for storage of images without express permission from the Headteacher.
- Access to these images are only for the school's staff and pupils for school purposes only and use on the schools website and VLN.
- Lee Goulding the Network Manager is responsible for the deletion of images no longer in use by the school or is the member of staff or pupil has left the school.

CCTV / Webcams

- The school has a large CCTV infrastructure for the safety and security of all persons on the site. The only people that have access to CCTV real-time viewing are SLT and the site management team.
- Any CCTV footage that is captured for security purposes is only available for viewing by the Headteacher, Site Manager and the Police.
- Webcams are only used in school as a learning resource within ICT lessons.

Misuse and Infringements

Complaints relating to e-Safety should be made to the e-Safety co-ordinator **Mr M. Edey** or Headteacher. Incidents should be logged and the Flowchart for e-Safety incidents should be followed (see appendix)

Handling E-Safety Complaints

- All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be reported immediately to the e-Safety co-ordinator and action in line with the Wigan Safeguarding Children Board e-Safety policy will be taken.
- Deliberate access to inappropriate material by any user will lead to the incident being logged by the e-Safety co-ordinator, depending on the seriousness of the offence: investigation by the Headteacher/LA, immediate suspension, possibly leading to dismissal and involvement of the police for very serious offences.
- Any staff misuse that suggests a crime has been committed, a child has been harmed or that a member of staff is unsuitable to work with children should be reported to the LADO within one working day in accordance with the Wigan Safeguarding Board Policy.
- Any complainant about staff misuse must be referred to the head teacher and if the misuse is by the head teacher it must be referred to the chair of governors in line with the Wigan Safeguarding Board Child Protection procedures.
- Pupils, parents and staff will be informed of the complaints procedure.

Equal Opportunities

Pupils with additional needs

The school endeavours to create a consistent message with parents for all pupils and this in turn should aid establishment and future development of the schools' e-Safety rules.

However, staff are aware that some pupils may require additional teaching including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of e-Safety issues.

Where a pupil has poor social understanding, careful consideration is given to group interactions when raising awareness of e-Safety.

Parental Involvement

Parental involvement is always welcomed at SHEVINGTON HIGH SCHOOL and we consider ourselves to have a good working and professional relationship with the parents of our pupils. We always try to encourage parents to have their say on any matter related to the school.

- Parents/Carers and pupils are actively encouraged to comment and contribute to adjustments or reviews of the schools e-Safety policy by emailing lgoulding@shevingtonhigh.org.uk

- Parents/Carers are asked to read through and sign any acceptable use agreements on behalf of the child on admission to school and any annual Internet/Email agreement forms.

- Parents/Carers are required to make a decision as to whether they consent to images of their child being taken/used in the public domain i.e. school website.

- The school disseminates information to parents relating to E-Safety where appropriate in the form of:

    - Information and celebration evenings
    - Posters
    - Website / Learning Platform postings
    - Newsletter Items
    - Learning platform training

Please sign, detach this sheet and return to the main office

Writing and Reviewing this Policy

This policy will be reviewed annually unless the school sees fit to add a change for security/safety reasons.

Review Procedure

There will be an on-going opportunity for staff to discuss with the e-Safety co-ordinator any issue regarding e-Safety that concerns them.

This policy will be reviewed annually unless the school sees fit to add a change for security/safety reasons.

The policy will be amended if new technologies are adopted or Central Government change the orders or guidance in any way.

This policy has been read, amended and approved by staff, Headteacher and governors _____.

Signed by: _____

Print Name: _____

Date: _____