**ACCEPTABLE NETWORK USE POLICY (E-SAFETY)**

Hele's School

## 1. Principles

1.1. New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning.

1.2. Young people should have an entitlement to safe internet access at all times.

1.3. This Acceptable Use Policy is intended to ensure:

- that young people are responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that School ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.

1.4. The School tries to ensure that students have good access to ICT to enhance their learning and, in return, expects the students to agree to be responsible users.

## 2. Practice

2.1. We provide filtered Internet access that blocks access to offensive sites and prevents offensive e-mails. Post16 students have a less restricted access to help with their studies.

2.2. We do not place named photographs of students on our web site.

2.3. We make the Internet available to students at lunchtimes and before/after School, in a supervised ICT room and/or in the Library.

2.4. We monitor and permanently log the web sites that staff and students access.

2.5. We issue a letter to all parents setting out our Acceptable Use Policy. Parents and students must sign and return a permission slip before those students can use the Internet.

2.6. Students are asked to report any misuse of School ICT systems, including physical damage, theft, bad language, distasteful pictures or other offensive material on the Internet in line with the Prevent Duty. Staff follow the procedures outlined in the Acceptable Use contract issued to parents/students each academic year.

2.7. It is forbidden for students to use School ICT systems or personal handheld technologies to:

- libel, harass, insult or attack others
- take or distribute images of anyone without their permission
- deliberately seek out or send offensive material in line with the Prevent Duty.

| | | | |
|---|---|---|---|
| Hele's School Policy No: | | Person/Group responsible: | **Network Manager** |
| Review Period: | **Annual** | Last review date: | March 2023 |
| Related documentation: | **IT network Policy (Staff)** | | |

- give out any personal details on the School Internet, including home address, phone number, picture, credit card or bank details
- arrange to meet someone with whom they have communicated on the Internet
- share or use another person's username and password
- use the Internet to play non-educational games or access chat sites without permission
- download any software files or install programmes from the Internet
- for online file sharing or video broadcasting
- Students who break these rules risk losing their Internet access, and additional sanctions are taken in line with the School Behaviour Management Policy.

**3. Roles and Responsibilities.**

3.1. Principal and Senior Leaders: The Principal and other members of the Senior Leadership Team are aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff.

3.2. Mr Edwards is the designated coordinator with responsibility for e-learning, working closely with Mr Kent, Network manager, and Mrs Crawford, Designated Safeguarding Lead. The coordinator will:

- take day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the School e-safety policies / documents
- ensure that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place
- provide training and advice for staff
- liaise with School ICT technical staff
- receive reports of e-safety incidents and create a log of incidents to inform and reports regularly to Senior Leadership Team

3.3. The network manager is responsible for ensuring that:

- the School's ICT infrastructure is secure and is not open to misuse or malicious attack
- users may only access the School's networks through a properly enforced password protection policy, in which passwords are regularly changed
- the use of the network is regularly monitored in order that any misuse can be reported to the ESafety Co-ordinator for investigation and action where necessary
- monitoring software systems are implemented and updated as agreed in Schools' policies

3.4. School staff are responsible for ensuring that:

- they have an up to date awareness of e-safety matters and of the current School e-safety policy and practices
- they have read, understood and signed the WeST staff Code of Conduct and KCSIE 22
- they report any suspected misuse or problem to the E-Safety Co-ordinator for investigation and action
- digital communications with students should be on a professional level and only
- students understand and follow the School e-safety and acceptable use policy
- they monitor ICT activity in lessons, extra-curricular and extended school activities
- they are aware of e-safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current School policies with regard to these devices in lessons. Where internet use is pre-planned students should be guided to sites checked as suitable

for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

- Staff are mindful of the Prevent strategy and act accordingly

3.5. Designated person for Child protection is trained in e-safety issues and is aware of the potential for serious child protection issues to arise from:

- the sharing of personal data access to illegal / inappropriate materials inappropriate on-line contact with adults / strangers
- potential or actual incidents of grooming
- cyber-bullying
- harmful sexual behaviours

3.6. Students are responsible for using the School ICT systems in accordance with the Student Acceptable Use Policy, which they will be expected to sign before being given access to School systems.

3.7. Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet and mobile devices in an appropriate way. The School will therefore take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website and information about esafety campaigns and literature. Parents and carers will be responsible for endorsing (by signature) the Student Acceptable Use Policy.

## 4. **Policy Statements**

### 4.1. Education – students

Whilst regulation and technical solutions are very important, their use must be balanced by educating students to take a responsible approach. The education of students in e-safety is therefore an essential part of the School's e-safety provision. Children and young people need the help and support of the School to recognise and avoid e-safety risks and build their resilience.

E-Safety education will be provided in the following ways:

- A planned e-safety programme will be provided as part of the ICT and PSHE curriculum - this will cover both the use of ICT and new technologies in School and outside School
- Key e-safety messages in assemblies and tutorial activities
- Students are taught in all lessons to be critically aware of the content they access on-line and are guided to validate the accuracy of information

### 4.2. Staff learning

- A planned programme of e-safety training will be made available to staff. It is expected that some staff will identify e-safety as a training need within the performance management process
- All new staff receive e-safety training as part of their induction programme, ensuring that they fully understand the School e-safety policy and Acceptable Use Policies
- The E-Safety Coordinator will provide advice, guidance and training as required to individuals

4.3. Technical – infrastructure / equipment, filtering and monitoring

The School ICT systems are managed in ways that ensure that the School meets the e-safety technical requirements. There are regular reviews and audits of the safety and security of School ICT systems Servers, wireless systems and cabling are securely located and physical access restricted

- All users have clearly defined access rights to School ICT systems
- All users are provided with a username and password by the Network Manager who will keep an up to date record of users and their usernames
- The "master / administrator" passwords for the School ICT system, used by the Network Manager are available to the Principal and kept in a secure place. Users will be made responsible for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security
- The School maintains and supports the filtering service provided by Smoothwall.
- School ICT technical staff regularly monitor and record the activity of users on the School ICT systems and users are made aware of this in the Acceptable Use Policy
- The School infrastructure and individual workstations are protected by up to date anti-virus software
- Personal data cannot be sent over the internet or taken off the School site unless safely encrypted or otherwise secured. Staff who need to do this in their particular role have encryption software installed on their laptops and are instructed in its use.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, handheld devices etc from accidental or malicious attempts which might threaten the security of the school systems and data.
- An agreed policy is in place regarding the downloading of executable files by users.
- An agreed policy is in place that allows staff to/forbids staff from installing programmes on school workstations/portable devices without contacting the Network Manager first.

4.5. Curriculum

- E-safety is a focus in all areas of the curriculum and staff reinforce e-safety messages in the use of ICT across the curriculum
- in lessons where internet use is pre-planned, students are guided to sites checked as suitable for their use
- Where students are allowed to freely search the internet, staff are vigilant in monitoring the content of websites visited
- It is accepted that from time to time, for good educational reasons, students may need to research topics (eg racism, drugs, discrimination) that normally result in internet searches being blocked. In such a situation, staff can request that the Network Manager can temporarily remove those sites from the filtered list for the period of study. Any request to do so, is audited with clear reasons for the need
- Students are taught in all lessons to be critically aware of the content they access on-line and be guided to validate the accuracy of information

4.6. Use of digital and video images – Photographic and Video

- When using digital images, staff should inform and educate students / pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they recognise the risks attached to publishing their own images on the internet eg on social networking sites
- Staff are allowed to take digital / video images to support educational aims, but must follow School policies concerning the sharing, distribution and publication of those images. Those images should only be taken on School equipment, the personal equipment of staff should not be used for such purposes
- Care should be taken when taking digital / video images that students / pupils are appropriately dressed and are not participating in activities that might bring the individuals or the School into disrepute
- Students must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include students / pupils will be selected carefully and will comply with good practice guidance on the use of such images
- Students' full names will not be used anywhere on a website or blog, particularly in association with photographs
- Parents or carers are given the opportunity to withdraw photographs of students that are published on the School website

4.7. Data Protection See Data Protection Policy

4.8. Communications

When using communication technologies the School considers the following as good practice:

- The official School email service may be regarded as safe and secure and is monitored. Users need to be aware that email communications may be monitored.
- Users must immediately report, to the nominated person – in accordance with the School policy, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email
- Any digital communication between staff and students or parents / carers (email, VLE etc) must be professional in tone and content

4.9. Unsuitable / inappropriate activities

Users shall not visit Internet sites, post, download, upload, communicate or pass on, material and comments that contain or relate to:

- Offensive materials: child sexual abuse images, promotion or conduct of illegal acts, eg under the child protection, obscenity, computer misuse and fraud legislation, adult material that potentially breaches the Obscene Publications Act in the UK, racist material, pornography, promotion of any kind of discrimination, promotion of religious hatred, threatening behaviour, or material undermining the Prevent Duty
- Using School systems to run a private business
- Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by Smoothwall and / or the School
- Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions
- Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)

- Creating or propagating computer viruses or other harmful files
- Carrying out sustained or instantaneous high volume network traffic (downloading / uploading files) that causes network congestion and hinders others in their use of the internet
- This also applies to students' personal handheld technologies to and from School and whilst on School premises

4.10. Responding to incidents of misuse

Any apparent or actual misuse which appears to involve illegal activity ie.

- child sexual abuse images
- adult material which potentially breaches the Obscene Publications Act
- criminally racist material or material that opposes British Values in line with the Prevent Duty.
- other criminal conduct, activity or materials will be reported initially to the E-Safety Coordinator.

Actions will be followed in line with the School procedures including reporting the incident to the police and the preservation of such evidence.

It is more likely that the School will need to deal with incidents that involve inappropriate rather than illegal misuse. Such incidents of misuse will be dealt with through the normal behaviour management policy.

**5. Review of Policy**

This policy is reviewed on an annual basis.

| | | | |
|---|---|---|---|
| Hele's School Policy No: | | Person/Group responsible: | **Network Manager** |
| Review Period: | **Annual** | Last review date: | March 2023 |
| Related documentation: | **IT network Policy (Staff)** | | |