T.I.M.E
Logic House
138 Central Street
St Helens
WA10 1UD
Tel: 01744 808040
enquiries@thisismyeducation.org.uk

Managing Director: Jillian Fairclough
jillianfairclough@thisismyeducation.org.uk

Facebook: This Is My Education

TIME

E-Safety Policy

This policy is in line with the Independent School Standards

Approved by:	Jillian Fairclough	**Date:**	September 2022

Next review due by:	September 2023

1. Introduction

The Internet is now regarded as an essential resource to support teaching and learning. The statutory curriculum requires students to learn how to locate, retrieve and exchange information using ICT. In delivering the curriculum, teachers need to plan to integrate the use of communications technology such as web-based resources and e-mail and mobile learning, such as phones. Computer skills are vital to access life-long learning and employment; indeed ICT is now seen as an essential life-skill.

Young people have access to the Internet from many places, home, school, friends' homes, libraries and in some cases mobile phones. Schools have a number of services to help ensure that curriculum use is safe and appropriate, however, access out of school does not usually have these services and has a range of risks associated with its use. Schools are ideally placed to help young people learn to become e-safe.

In line with other This Is My Education (TIME) policies that protect students from other dangers, there is a requirement to provide students with as safe an Internet environment as possible and a need to teach them to be aware of and respond responsibly to the risks.

2. Core Principles of Internet Safety

The Internet is becoming as commonplace as the telephone or TV and its effective use is an essential life-skill. Unmediated Internet access brings with it the possibility of placing of students in embarrassing, inappropriate and even dangerous situations. Schools need a policy to help to ensure responsible use and the safety of students.

The TIME E-Safety Policy is built on the following five core principles:

2.1: Guided educational

Significant educational benefits should result from curriculum Internet use including access to information from around the world and the abilities to communicate widely and to publish easily. Curriculum Internet use should be planned, task-orientated and educational within a regulated and

managed environment. Directed and successful Internet use will also reduce the opportunities for activities of dubious worth.

2.2: Risk assessment

21st century life presents dangers including violence, racism and exploitation from which children and young people need to be protected. At the same time they must learn to recognise and avoid these risks – to become "Internet Wise". Schools need to ensure that they are fully aware of the risks, perform risk assessments and implement a policy for Internet use. Students need to know how to cope if they come across inappropriate material.

Students may obtain Internet access in youth clubs, libraries, and public access points and in homes. Ideally a similar approach to risk assessment and Internet safety would be taken in all these locations, although risks do vary with the situation.

2.3: Responsibility

Internet safety depends on staff, schools, governors, advisers, parents and, where appropriate, the students themselves taking responsibility for the use of Internet and other communication technologies such as mobile phones. The balance between educating students to take a responsible approach and the use of regulation and technical solutions must be judged carefully. There are a number of technical solutions to help limit Internet access, though; it is the appropriateness and consistency of the school's e-safety policy that is of overriding importance.

2.4: Regulation

The use of a finite and expensive resource, which brings with it the possibility of misuse, requires regulation. In some cases, access within schools must simply be denied, for instance unmoderated chat rooms present immediate dangers and are usually banned. Fair rules, clarified by discussion and prominently displayed at the point of access will help students make responsible decisions.

2.5: Appropriate strategies

This document describes strategies to help to ensure responsible and safe use. They are based on limiting access, developing responsibility and on guiding students towards educational activities. Strategies must be selected to suit the school situation and their effectiveness monitored. ***There are no straightforward or totally effective solutions and staff, parents and the students themselves must remain vigilant.***

3. Why is Internet use important?

- The purpose of Internet use in school is to raise educational standards, to promote student achievement, well being and to

support the professional work of staff and to enhance the school's management information and business administration systems.
- Internet use is a part of the statutory curriculum and a necessary tool for staff and students.
- Internet access is an entitlement for students who show a responsible and mature approach to its use.
- The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide students with quality Internet access as part of their learning experience.

4. How will Internet use enhance learning?

There is now increased computer and Internet access both within school and at home. Developing good practice in Internet use as a tool for teaching and learning is clearly essential. Teachers need to help students learn to become "web literate", for example, understand the need to keep personal information safe and to appreciate that as with all publishing a critical awareness of validity and bias is important.

- The school Internet access will be designed expressly for educational use and will include filtering appropriate to the age of students.
- Students will learn appropriate Internet use and be given clear objectives for Internet use.
- Staff should guide students in online activities that will support the learning outcomes planned for the students' age and maturity.
- Students will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

5. How will Internet access be authorised?

Internet access for students should be seen as an entitlement on the basis of educational need and an essential resource for staff.

6. How will filtering be managed?

Despite careful design, filtering systems cannot be completely effective due to the speed of change of web content. A filtering system is in place via our ICT supports students as part of a supervised project, might need to access adult materials; for instance a course text or set novel might include references to sexuality. Subject teachers might need to research areas including drugs, medical conditions, bullying, racism or harassment. In such cases, legitimate use should be recognised and restrictions removed temporarily. TIME IT use a filtering software, SmoothWall which blocks unsuitable content.

- If staff or students discover unsuitable sites, the URL (address) and content must be reported to the Head Teacher via the ICT co-ordinator.
- Any material that TIME staff believes is illegal must be referred to the Internet Watch.

7. How will the risks be assessed?

In common with other media such as magazines, books and video, some material available via the Internet is unsuitable for students. TIME will take all reasonable precautions to ensure that users access only appropriate 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 school computer.

The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.

Methods to identify, assess and minimise risks will be reviewed regularly. The Teacher In Charge will ensure that the Internet policy is implemented and compliance with the policy monitored.

8. Managing Content

8.1 How will students learn to evaluate Internet content?

Information received via the web, e-mail or text message requires good information-handling skills. In particular it may be difficult to determine origin and accuracy, as the contextual clues present with books or TV may be missing or difficult to read. Students need to understand that some content is deliberately misleading, while some is/may be unsuitable from purely a reading-age perspective. Ideally inappropriate material would not be visible to students using the web but this is not easy to achieve and cannot be guaranteed. It is a sad fact that students may occasionally be confronted with inappropriate material, despite all attempts at filtering. Students should be taught what to do if they experience material that they find distasteful, uncomfortable or threatening. For example: to close the page and report the URL to the teacher or ICT manager for inclusion in the list of blocked sites. More often, students will be judging reasonable material but need to select that which is relevant to their needs, for instance to answer a homework question. Students should be taught research techniques and encouraged to question the validity, currency and origins of information – looking for the author's name, date of revision and whether others link to the site is a start. Students should also use alternative sources of

information for comparison purposes. Effective guided use should also reduce the opportunity students have for exploring undesirable areas.

Using Internet derived materials in students' own work requires at least an understanding that straight copying is worth little without a commentary that demonstrates the selectivity used and evaluates significance. Respect for copyright and intellectual property rights, and the correct usage of published material will be taught.

- Any Internet derived materials by staff and by students must comply with copyright law.
- A nominated person will be responsible for permitting and denying additional websites as requested by colleagues.
- Students will be taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work.

10. Communication

10.1 Managing e-mail

At Key Stage 4 emailing is taught through ICT lessons. Students will learn how to send and receive and to use email etiquette. The students themselves will not have their own email accounts.

10.2 On-line communications and social networking.

TIME have a key role to teach young people about the importance of keeping personal information safe, not posting comments and pictures of other people that may cause upset and to communicate in an appropriate manner. The use of online communications and social networking is not permitted in school.

10.3 Mobile technologies

Many emerging communications technologies offer the potential to develop new teaching and learning tools. Mobile communications, wide Internet access and online learning need to be evaluated to assess risks, to establish benefits and to develop good practice.

The internet can enhance learning. It is how students are taught to use the internet appropriately and safely is important, e.g. to keep their registration details safe, to know that the information they save in these environments is bound within the school's code of conduct are all important. Though this may seem obvious to an adult, it may not be to all students and is an important issue to clarify with students.

Mobile phones within school are a growing concern for teachers. Older students using them to take images of students and teachers without consent, posting them onto the web afterwards can cause a great deal

of upset and distress. A good start is to educate students with little knowledge or who may not appreciate the consequences of their actions that the posting of images without consent and which cause distress and harassment can have legal consequences. Legal guidance relating to cyber bullying using mobile phones and online services is outlined during ICT lessons. Each base has their own mobile phone policy:

- at TIME students hand their mobile phones in at the begin of the day and have them

Failure to follow the policy will result in a disciplinary procedure.

11. Introducing the Policy to Students

Many students are very familiar with Internet use and the culture that surrounds it. As part of the school's e-safety teaching and awareness-raising it would be sensible to discuss the key features with students / students as appropriate for their age. Students may need to be reminded of the school rules at the point of Internet use. During the induction of a new young person to TIME they will be told that their Internet use will be monitored.

A module on responsible Internet use and e-safety is included in the curriculum covering both school and home use. This will include the necessity of keeping personal information safe, how to use mobile technologies appropriately and using online communication appropriately. Parents receive a letter to inform them that their child has taken part in eSafety lessons and a guidance at home leaflet is enclosed. TIME use CEOP's ThinkUKnow 14-16 materials as a teaching tool.

12. Parents and E-Safety

Internet use in students' homes is increasing rapidly, encouraged by offers of free access and continual media coverage. Unless parents are aware of the dangers, students may have unrestricted access to the Internet. Information will be provided to parents from TIME in the form of Parental Guidance leaflets about how to ensure they can work with their children to ensure this resource is used appropriately at home.

13. Consulting with Staff and their inclusion in the E-safety Policy

It is important that teachers and learning support assistants are confident to use the Internet in their work. By having a clear set of acceptable use rules that are fairly and consistently applied generally have fewer incidences of misuse and online bullying incidences. Staff should be given opportunities to discuss the issues and develop appropriate teaching strategies. It would be unreasonable, for instance, if cover staff or supply

staff were asked to take charge of an Internet activity without preparation or clarification and discussion may be required.

All school staff need to be aware that they are subject to the same conditions as any TIME employee on Internet misuse. All staff including teachers, supply staff, classroom assistants and support staff, will be provided with the School Internet Policy, and its importance explained. Staff should be aware that Internet traffic is monitored and reported by THE Head Teacher and can be traced to the individual user. Discretion and professional conduct is essential.

14. How will complaints be handled?

Teachers must know how and where to report incidents, this would be to Teacher In Charge. Prompt action will be required if a complaint is made. The facts of the case will need to be established, for instance whether the Internet use was within or outside school. A minor transgression of the rules may be dealt with by the teacher as part of normal class discipline. Other situations could potentially be serious and a range of sanctions will be required, linked to the school's behaviour policy. All record of the incident should be kept, e.g. e-mails saved or printed, text messages saved etc. Complaints of a child protection nature must be dealt with in accordance with the schools Child Protection procedures this should also be recorded on CPOMS.

Responsible Internet Use

Rules for Staff and Students

The computer system is owned by the school. This Responsible Internet Use statement helps to protect students, staff and the school by clearly stating what use of the computer resources is acceptable and what is not.

- Irresponsible use may result in the loss of Internet access.
- Network access must be made via the user's authorised account and password, which must not be given to any other person.
- School computer and Internet use must be appropriate to the student's education or to staff professional activity.
- Copyright and intellectual property rights must be respected.
- E-mail should be written carefully and politely, particularly as messages may be forwarded or printed and be seen by unintended readers. Users are responsible for e-mail they send.
- Attempts made to bypass the Internet filtering system will breach the acceptable user policy and will be reported to the headteacher for action.
- The school ICT systems may not be used for private purposes, unless the Teacher In Charge has given permission for that use.
- Use for personal financial gain, gambling, political purposes or advertising is not permitted.
- ICT system security must be respected; it is a criminal offence to use a computer for a purpose not permitted by the system owner.
- The school may exercise its right to monitor the use of the school's computer systems, including access to web-sites, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the school's computer system is or may be taking place, or the system is or may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

Responsible Internet Use

These rules help us to be fair to others and keep everyone safe.

- I will ask permission before using the Internet.
- I will use only my class network login and password, which is secret.
- I will only open or delete my own files.
- I understand that I must not bring into school and use software or files without permission.
- I understand that I must never give my home address or phone number, or arrange to meet someone.
- If I see anything I am unhappy with then I will tell a teacher immediately.
- I understand that the school may check my computer files and the Internet sites I visit.
- I understand that if I deliberately break these rules, I may not be allowed to use the Internet or computers.
- I will take part in eSafety lessons.

Young Person Name	
Young Person Signature	
Date	

Parent/Carer's Consent for Internet Access

I have read and understood the school rules for responsible Internet use and give permission for my son / daughter to access the Internet.

I understand that the school will take all reasonable precautions to ensure students cannot access inappropriate materials.

I understand that the school cannot be held responsible for the nature or content of materials accessed through the Internet.

I agree that the school is not liable for any damages arising from use of the Internet facilities.

Name of Young Person:
Parent/Carer Signature:
Please print name:
Date:

TIME ICT Agreement Policy

Guideline for all Users of the School Network

Access to the school network and Internet is provided for you to carry out recognised schoolwork. This provision will only be made on the understanding that you agree to follow these guidelines.

- Computer (file) storage areas will be treated as school property. ICT staff may look at files and communications to ensure that the system is being used responsibly. Users should not expect their work to be private.
- You should also be aware that a member of the ICT staff could view your computer screen, from the school network without your knowledge, at any time.
- Users are responsible for good behaviour. General school rules apply whilst using the computers.
- Eating, drinking or the use of aerosol sprays near a computer may cause serious damage and are strictly prohibited.
- Do not use another person's password.
- Do not reveal your password to anyone. If you think someone knows your password, then ask for it to be changed.
- Programs must not be loaded or installed on a computer except by ICT Support Staff. Do not bring programs in on removable media, e-mail or download them from the Internet.
- The Internet is provided for users to conduct genuine research and communicate with others. All the sites you visit are recorded.
- During lessons, teachers will guide students toward appropriate materials. Outside lessons, families bear this responsibility.

<u>You are not permitted to:</u>

- Download any files without permission.
- Use Social Networking sites.
- Use Instant Messengers (e.g. AOL IM, Yahoo Pager, MSN)
- Use Chat, play games, use mobile ring tones sites or SMS sites.
- Use web mail.
- Use obscene or offensive language, (online, e-mail and phone text) remember communication should be polite to maintain the good reputation of the school.
- Take and use images of students and or staff without their prior consent.
- Seek out any offensive material.
- Complete mailing lists or subscription forms on the Internet for personal use.
- Violate copyright laws. (Never copy and make use of any material without giving credit to the author. Copyright, Designs and Patents Act 1988).

Sanctions

Violations of the above rules will result in either a temporary or permanent ban of Internet and/or network use, ranging from a 1-week Internet ban, to total network privileges removed.

Serious offences will be addressed as required.

You are reminded that you are always subjected to the Data Protection Act 1998, Computer Misuse Act 1990 and Copyright, Designs and Patents Act 1988.

The School reserves the right to seek remuneration from parents of students who cause malicious damage to ICT equipment.

We agree to the terms and conditions of the TIME Students ICT Agreement Policy'.

Student Name			
Student signature		Date	
Parent/Carer signature		Date	

15. Notes on the Legal Framework

The Computer Misuse Act 1990 makes it a criminal offence to gain access to a computer without permission. The motivation could be the technical challenge, data theft or to damage the system or data. The Rules for Responsible Internet Use remind users of the ownership of the school computer system.

Monitoring of data on a school network could contravene Article 8 of the European Convention of Human Rights and Fundamental Freedoms, e.g. the right to respect for private and family life, which is protected by the Human Rights Act 1998. The Telecommunications (Lawful Practice) (Interception of Communications) Regulations 2000 also limit monitoring. The 2000 Regulations apply to all forms of electronic monitoring and interception irrespective of whether the material monitored is generated by private use or in the course of the school's day-to-day activities.

A school may only monitor authorised private use of a computer system if it can justify monitoring on the basis that it is lawful, necessary and in the interests of, amongst other things, the protection of health or morals or for the protection of the rights and freedoms of others. Schools should ensure that the monitoring is not out of proportion to the harm that could be done if the monitoring did not take place.

Schools could start by banning private use of a school's computer system, but then allow private use following the signing of an agreement to use the equipment under the conditions as laid out by the school. (A copy of the Council's policy is included in section 15). The Rules for Responsible Internet Use, to which every user must agree, contain a paragraph that should ensure users are aware that the school is monitoring Internet use.

In order to defend claims that it has breached either the 2000 Regulations or the Human Rights Act 1998, a school should devise procedures for monitoring, ensure monitoring is supervised by a senior manager and maintain a log of that monitoring. For example, each school can review the websites visited by the school each day / week / month. Though this is not user specific it does allow a degree of monitoring to be conducted. All schools are also able to monitor school e-mail.

Cyber-stalking and Harassment (http://wiredsafety.org/gb/stalking/index.html)

Under Section 1 of the Malicious Communications Act 1998 it is an offence to send an indecent, offensive or threatening letter, electronic communication or other article to another person and under Section 43 of the Telecommunications Act 1984 it is a similar offence to send a telephone message which is indecent, offensive or threatening. In both cases the offence is punishable with up to six months' imprisonment and/or a fine of up to £5000. As the Malicious Communications Offence is more wide-ranging than the Telecommunications offence it is more likely to be used by the Police than the Telecommunications Act offence.

In most cases involving malicious communications or cyber-stalking however there will be more than one offensive or threatening letter or telephone call and

therefore the police will often choose to charge the offender with an offence contrary to Section 2 of the Protection from Harassment Act 1997; also punishable with up to six months' imprisonment. Part of the reason for using this charge is that when someone is convicted of an offence under the Protection from Harassment Act 1997 the court can make a Restraining Order preventing them from contacting their victim again. Breach of a Restraining Order is punishable with up to five years' imprisonment. A Restraining Order cannot be imposed for a conviction under the Malicious Communications or Telecommunications Acts.

If the e-mails, cyber-stalking etc. causes the victim to fear that violence will be used against them then the police can choose to charge the offender with an offence contrary to Section 4 of the Protection from Harassment Act 1997 which is punishable with up to five years' imprisonment and also allows the court to make a Restraining Order.

If the e-mails, cyber-stalking etc. is racist in nature or motivated by religious hostility then charges could be brought of Racially or Religiously-Aggravated Harassment contrary to Sections 32(1)(a) or 32(1)(b) of the Crime and Disorder Act 1998. If convicted offenders could face up to 7 years' imprisonment.

The fact that an offensive telephone call, letter e-mail etc. may be received in the course of work and have been sent by a work colleague or manager does not justify the message or prevent it being an offence. Offensive messages sent within the workplace can still constitute criminal offences. In addition they may justify a claim for constructive dismissal and compensation under employment law.

In many situations the recipient of malicious messages knows who the sender is. It may be a former partner or a relative which may mean that the victim is reluctant to involve the police. In those circumstances the victim could consider taking out an Injunction under Section 3 of the Protection from Harassment Act 1997. However we would always advise informing the police especially if the messages are in any way threatening. Even if the police decide not to prosecute they may give the offender a formal warning which could be used in evidence if they repeated their behaviour in future.

In addition to criminal prosecutions victims of harassment can sue the offender under Section 3 of the Protection from Harassment Act 1997 for damages arising out of the anxiety caused by the harassment and any financial loss it caused.

…… Head Teacher

…… Chair of Management Committee

…… Date