West Hill School

Aiming High Since 1927

ICT E-Safety Policy

Item	Author/Owner	Date Written	Approved by	Date Approved
1.0	Mr A. O'Brien	Oct 2023	Board of Trustees	Nov 2023
1.1	Mr P. Gillon	Nov 2024	Board of Trustees	Nov 2024
1.2	Mr A. O'Brien	Jun 2025	Board of Trustees	July 2025
1.3	Mr A. O'Brien	Jun 2026	Full Board of Trustees	July 2026

Contents

Introduction

West Hill School supports a culture of whole school awareness, through policies, procedures and training that provide for a safe IT environment.

The educational benefits of technologies, such as the internet and email, Virtual Learning Environments, weblogs, smartphones, podcasting and video conferencing cannot be underestimated. These help to motivate children in their learning, equipping them with essential skills for the future, as well as enabling access to information which might not otherwise have been available.

All users of the IT systems at West Hill (staff, students, guests, contractors) should expect it to be a safe place and every precaution to have been taken to restrict access to any inappropriate or illegal content. In equal measure, users of the systems are expected to behave appropriately regarding their own and other's safety when working with the IT systems provided. This policy sets out the intentions of the school for its IT provision and the expectations of its users.

The E–Safety Policy is part of the school suite of IT and Safeguarding Policies. It also relates to other policies including those for behaviour, anti-bullying, personal, social and health education (PSHCE) and for citizenship.

The E-Safety Policy and its implementation will be reviewed annually. Our E-Safety Policy has been written by school to support the safe use of IT through a culture of whole school awareness, utilising policies, procedures and training.

The school has appointed an E-Safety Team, consisting of:

- Designated Safeguarding Lead
- Network Manager
- Trustee with Child Safeguarding Responsibilities

West Hill School Thompson Cross, Stamford Street, Stalybridge, Cheshire SK15 1LX T: 0161 338 2193 E: admin@westhillschool.co.uk W: www.westhillschool.co.uk

Managing Information Systems

It is important to review the security of the whole system from user to internet. This is a major responsibility that includes not only the delivery of essential learning services but also the personal safety of staff and students.

The school has a responsibility to ensure that IT is used and managed legitimately, and the security of the school information systems and users will be reviewed regularly, as laid down in the school IT Security Policy.

All users of the network, with the exception of students, must complete the Cyber Security Training for school staff, published by the National Cyber Security Centre before being granted access to the network.

Published Content

The school makes use of the school website, Facebook and Instagram to promote and publish information about the school, its staff, students and events.

The publishing of content to these is limited to the staff who vet the content prior to publication to ensure that it complies with school guidelines for publications including respect for intellectual property rights and copyrights.

Publication of Student Images and Work

Still and moving images and sounds add liveliness and interest to a publication, particularly when students are included. Nevertheless, the security of staff and students is paramount.

To secure the safe management of the publication of student images and work, a number of strategies are identified and their application should be followed.

Before the publication of any student image or material, consent must be sought from the parent/carer. In most instances, consent is already granted through the student data collection sheet. This must be checked before any publication is made. This is especially important when students are Looked After Children.

Details of consents are on the student's details page on SIMS under Section 12, Parental Consent. If you have any additional queries, you should contact the Designated Safeguarding Lead, Network Manager or the Business Manager/DPO.

Photographs can be used providing no name can be linked to a particular student, i.e. a group photograph is taken and names are published, but not in the order of the photograph. If a photograph of a single student is used it is recommended that no reference be made to their name.

Further information can be found at:

Taking photos in schools | ICO

West Hill School Thompson Cross, Stamford Street, Stalybridge, Cheshire SK15 1LX T: 0161 338 2193 E: admin@westhillschool.co.uk W: www.westhillschool.co.uk

Social Networking, Social Media and Personal

Parents and teachers need to be aware that the Internet has online spaces and social networks which allow individuals to publish unmediated content.

Social networking sites can connect people with similar or very different interests. Users can be invited to view personal spaces and leave comments, over which there may be limited or no control.

For responsible adults, social networking sites provide easy to use, free facilities; although often advertising intrudes and may be dubious in content.

Students should be encouraged to think about the ease of uploading personal information, the associated dangers and the difficulty of removing an inappropriate image or information once published.

All staff should be made aware of the potential risks of using social networking sites or personal publishing either professionally with students or personally. They should be made aware of the importance of considering the material they post, ensuring profiles are secured and how publishing unsuitable material may affect their professional status.

Examples include: blogs, wikis, social networking, forums, bulletin boards, multi-player online gaming, chat rooms, instant messenger apps and others.

Please refer to the Staff Code of Conduct in the ICT User Guide. This states that instant messaging and social networking is not acceptable with current or ex-students under the age of 18. Breaches of this will be investigated and may lead to disciplinary procedures.

Staff must also be aware of their conduct within the scope of 'Part Two: Personal and professional conduct' of the Teacher Standards set out by the government when using social media.

For the above reasons it has been decided that access to these sites (with the exception of Instagram and Facebook for school related posts) in school will not be permitted for all staff and students.

Emerging Technologies

Many emerging technologies offer the potential to develop new teaching and learning opportunities, including the use of mobile communications, internet access, collaboration and multimedia tools.

The safety and effectiveness of these communications depends on users being trusted and identifiable. As new technologies and systems emerge, staff must consult with the Network Manager who will consider whether such systems can be managed in order to ensure that safeguarding procedures can always be followed.

West Hill School Thompson Cross, Stamford Street, Stalybridge, Cheshire SK15 1LX T: 0161 338 2193 E: admin@westhillschool.co.uk W: www.westhillschool.co.uk

Data Retention

At all times the content of areas used by staff, e.g. email and file storage, can be accessed and inspected for policy compliance by the Network Manager as directed by the Designated Safeguarding Lead or members of SLT. All files and emails are retained by the school after the end of an individual's employment in line with the school's Data Protection Policy.

Policy Implementation

This section summarises how the E-safety policy will be implemented across the school.

Internet Access

The internet and email facilities are provided to allow research to be conducted and as a means of communication with others. Access to these facilities is a privilege and not a right. Parental/carer consent is obtained via student data collection. This allows the student to use the internet and email and is confirmed each year by the agreement in the West Hill School app from Weduc.

Risk Assessment

The school will take all reasonable precaution to ensure that users access only appropriate material. However, owing to the global and connected nature of internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer. The school cannot accept liability for material accessed or any consequences resulting from internet use.

However, school does employ the use of robust monitoring systems to reduce and manage the risks present. These are updated in accordance with industry guidelines.

The school will audit ICT use to establish that the E-Safety Policy is adequate and that the implementation is appropriate.

Handling of E-Safety Incidents

Minor incidents may be dealt with by a member of staff but should still be reported to the safeguarding team. Other situations could potentially be serious and a range of sanctions will be required, linked to the school's Disciplinary Policy.

Potential safeguarding or legal issues must be referred to the school's Designated Safeguarding Lead. Advice on dealing with illegal use can be obtained from the Police and authorities, if necessary. Please refer to the flow chart contained in this policy for additional guidance.

West Hill School Thompson Cross, Stamford Street, Stalybridge, Cheshire SK15 1LX T: 0161 338 2193 E: admin@westhillschool.co.uk W: www.westhillschool.co.uk

Cyberbullying

Cyberbullying is defined as:
Cyberbullying, or online bullying, can be defined as the use of technologies by an individual or by a group of people to deliberately and repeatedly upset someone else.
(Cyberbullying - UK Safer Internet Centre, June 2025)

It is essential that young people, school staff and parents/carers understand how cyberbullying is different from other forms of bullying, how it can affect people and how to respond and combat misuse. Promoting a culture of confident users will support innovation and safety.

Cyberbullying along with all forms of bullying will not be tolerated at West Hill School. Full details are set out in the school's Anti-Bullying Policy. All incidences of cyberbullying reported to the school will be recorded and investigated by the Designated Safeguarding Lead.

Sanctions for those involved in cyberbullying may include:

- The bully will be asked to remove any material deemed to be inappropriate or offensive
- A service provider may be contacted to remove content
- Internet access will be suspended for a period of time
- Computer access may be suspended for a period of time
- Parents/carers may be informed
- The police and Children's Social Care will be contacted if a criminal offence is suspected.

Repeat offences will lead to further sanctions as outlined in the Anti-Bullying Policy.

The Department for Education (DfE) and Childnet have produced resources and guidance that can be used to give practical advice on Cyberbullying:
What is cyberbullying and what can I do about it? | Childnet (June 2025)

Learning Platforms/Environments

An effective learning platform or learning environment can offer schools a wide range of benefits to teachers, students, parents as well as support management and administration. It can enable students and teachers to collaborate in and across schools, can share resources and tools for a range of topics, create and manage digital content and students can develop online and secure e-portfolios.

The learning platforms/environments will be managed to allow only current staff, students and parents/carers access. All users should be aware that SLT and staff will monitor the usage of the learning platform in all areas, in particular message and communication tools and publishing facilities.

All users will be mindful of copyright issues and will upload only appropriate content onto the learning platform.

West Hill School Thompson Cross, Stamford Street, Stalybridge, Cheshire SK15 1LX T: 0161 338 2193 E: admin@westhillschool.co.uk W: www.westhillschool.co.uk

Communicating the Policy

This policy has been designed with Trustees, staff, students and parents/carers in mind. The contents of this should be shared with all these stakeholders and complied with.

It is important that all users feel confident to use ICT. The school E–Safety Policy will only be effective if everyone subscribes to its values and methods. Staff should be given opportunities to discuss the issues and develop appropriate teaching strategies. It would be unreasonable, for instance, if cover or supply staff were asked to take charge of an internet activity without preparation.

Through the school website we provide parents/carers with information to help them to understand the risks involved and how to access a range of materials and other information to assist them. They can also contact the school for advice or to raise any concerns that they may have. These will be passed to the most relevant person for action.

Legal Framework

This section is designed to inform users of potential legal issues relevant to the use of electronic communications. It is not professional advice.

Many young people and indeed some staff use the internet regularly without being aware that some of the activities they take part in are potentially illegal. The law is continually developing and changes occur frequently.

Counter-Terrorism and Security Act 2015

From 1 July 2015 all schools, registered as Early Years childcare providers and registered Later Years childcare providers are subject to a duty under section 26 of the Counter-Terrorism and Security Act 2015, in the exercise of their functions, to have “due regard to the need to prevent people from being drawn into terrorism”. This duty is known as the Prevent duty. It applies to a wide range of public-facing bodies. Bodies to which the duty applies must have regard to the statutory guidance. Paragraphs 57-76 of the guidance are concerned specifically with schools and childcare providers.

Racial and Religious Hatred Act 2006

This act makes it a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

Criminal Justice Act 2003

Section 146 of the Criminal Justice Act 2003 came into effect in April 2005, empowering courts to impose tougher sentences for offences motivated or aggravated by the victim's sexual orientation in England and Wales.

West Hill School Thompson Cross, Stamford Street, Stalybridge, Cheshire SK15 1LX T: 0161 338 2193 E: admin@westhillschool.co.uk W: www.westhillschool.co.uk

Sexual Offences Act 2003

It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). This can include images taken by and distributed by the child themselves (often referred to as "Sexting"). **A person convicted of such an offence may face up to 10 years in prison.**

The offence of grooming is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence.

Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust (typically, teachers, social workers, health professionals, Connexions staff etc. fall in this category of trust) to engage in sexual activity with any person under 18.

Any sexual intercourse with a child under the age of 13 commits the offence of rape. N.B. Please refer to the "Children & Families: Safer from Sexual Crime" document included in the "Child Protection – Essential Guidance for all Staff" file located in the reception office.

More information about the 2003 Act can be found at www.teachernet.gov.uk

Communications Act 2003 (section 127)

Sending by means of the internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment.
This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

Data Protection Act 2018

The act requires anyone who handles personal information to notify the Information Commissioner's Office of the type of processing it administers, and must comply with important data protection principles when treating personal data relating to any living individual. The act also grants individuals rights of access to their personal data, compensation and prevention of processing.

The Computer Misuse Act 1990 (sections 1-3)

Regardless of an individual's motivation, the act makes it a criminal offence to:

West Hill School Thompson Cross, Stamford Street, Stalybridge, Cheshire SK15 1LX T: 0161 338 2193 E: admin@westhillschool.co.uk W: www.westhillschool.co.uk

-Gain access to computer files or software without permission (for example using someone else's password to access files);
-Gain unauthorised access, as above, to commit a further criminal act (such as fraud); or
-Impair the operation of a computer or program (for example caused by viruses or denial of service attacks).

UK citizens or residents may be extradited to another country if they are suspected of committing any of the above offences.

Malicious Communications Act 1988 (section 1)

This legislation makes it a criminal offence to send an electronic message (email) that conveys indecent, grossly offensive, threatening material or information that is false; or is of an indecent or grossly offensive nature if the purpose was to cause a recipient to suffer distress or anxiety.

Copyright, Design and Patents Act 1988

Copyright is the right to prevent others from copying or using an author's "work" without permission.

The material to which copyright may attach (known in the business as "work") must be the author's own creation and the result of some skill and judgement. It comes about when an individual expresses an idea in a tangible form. Works such as text, music, sound, film and programs all qualify for copyright protection. The author of the work is usually the copyright owner, but if it was created during the course of employment it belongs to the employer.
It is an infringement of copyright to copy all or a substantial part of anyone's work without obtaining the author's permission. Usually, a licence associated with the work will allow a user to copy or use it for limited purposes. It is advisable always to read the terms of a licence before you copy or use someone else's material.

It is also illegal to adapt or use software without a licence or in ways prohibited by the terms of the software licence.

Public Order Act 1986 (sections 17-29)

This act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material, with a view of releasing it, a criminal offence.

Obscene Publications Act 1959 and 1964

Publishing an "obscene" article is a criminal offence. Publishing includes electronic transmission.

Protection from Harassment Act 1997

A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows, or ought to know, amounts to harassment of the other.

West Hill School Thompson Cross, Stamford Street, Stalybridge, Cheshire SK15 1LX T: 0161 338 2193 E: admin@westhillschool.co.uk W: www.westhillschool.co.uk

A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows, or ought to know, that his course of conduct will cause the other so to fear on each of those occasions.

Regulation of Investigatory Powers Act 2000
The Regulation of Investigatory Powers Act 2000 (RIP) regulates the interception of communications and makes it an offence to intercept or monitor communications without the consent of the parties involved in the communication. The RIP was enacted to comply with the Human Rights Act 1998.

The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, however, permit a degree of monitoring and record keeping, for example, to ensure communications are relevant to school activity or to investigate or detect unauthorised use of the network. Nevertheless, any monitoring is subject to informed consent, which means steps must have been taken to ensure that everyone who may use the system is informed that communications may be monitored.

Covert monitoring without informing users that surveillance is taking place risks breaching data protection and privacy legislation.

Criminal Justice and Immigration Act 2008

Section 63 offence to possess “extreme pornographic image” 63 (6) must be “grossly offensive, disgusting or otherwise obscene”. 63 (7) this includes images of “threats to a person life or injury to anus, breasts or genitals, sexual acts with a corpse or animal whether alive or dead” must also be “explicit and realistic”. Penalties can be up to 3 years imprisonment.

Education and Inspections Act 2006

Education and Inspections Act 2006 outlines legal powers for schools which relate to cyberbullying/bullying:

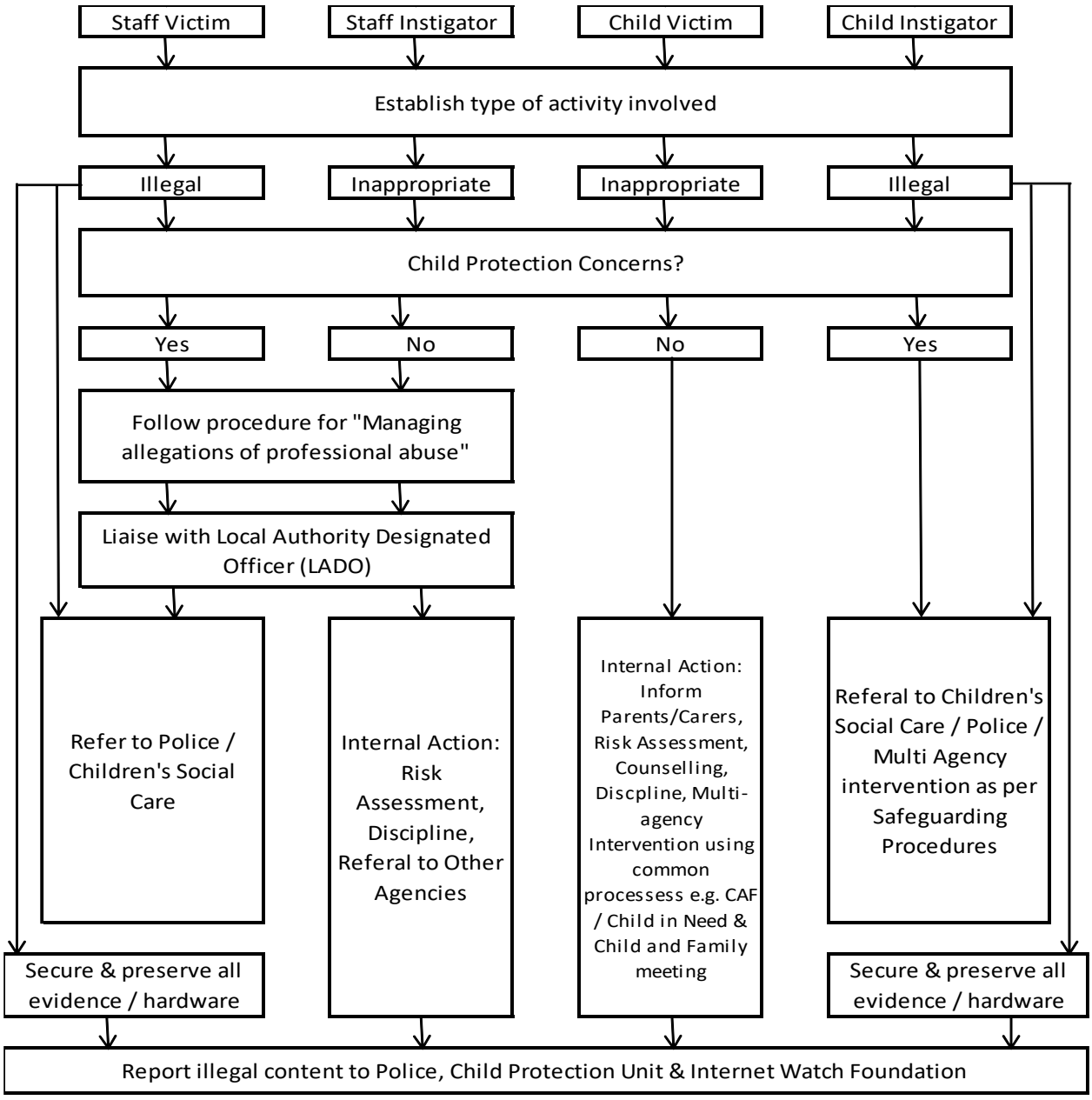
Headteachers have the power “to such an extent as is reasonable” to regulate the conduct of students off site. School staff are able to confiscate items such as mobile phones when they are being used to cause a disturbance in class or otherwise contravene the school Behaviour/Anti-Bullying Policy.

Telecommunications Act 1984

The transmission of an obscene or indecent image from one computer to another via a ‘public telecommunications system’ is an offence under section 43 of this Act. For traditional mail, the same sort of offence is created under the Post Office Act 1953.

West Hill School Thompson Cross, Stamford Street, Stalybridge, Cheshire SK15 1LX T: 0161 338 2193 E: admin@westhillschool.co.uk W: www.westhillschool.co.uk

Reporting of Incidents



West Hill School Thompson Cross, Stamford Street, Stalybridge, Cheshire SK15 1LX T: 0161 338 2193 E: admin@westhillschool.co.uk W: www.westhillschool.co.uk