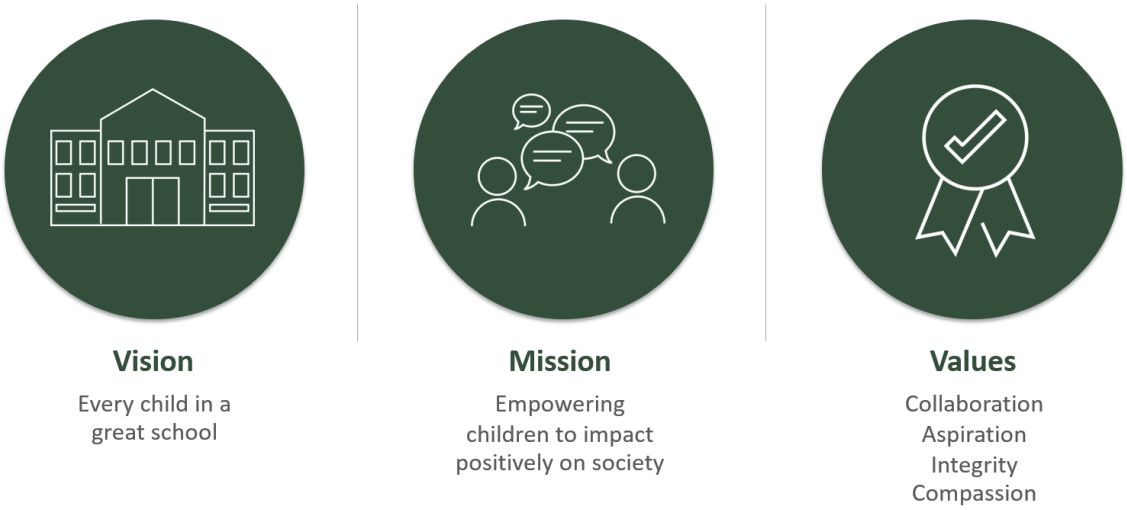
WeST Online Safety Policy

Person(s) responsible for updating the policy:	Director of Safeguarding / School online safety lead
Date approved by Trustees:	
Date of next review:	March 2027

Mission, Vision and Values



WeST Core Values

WeST holds four core values which underpin the engagement, motivation and retention of employees, no matter what their role in the organisation.

- **Collaboration**
  Creating a shared vision and working effectively across boundaries in an equitable and inclusive way to skillfully influence and engage others. Building and securing value from relationships, developing self and others to achieve positive outcomes.
- **Aspiration**
  Having high expectations, modelling the delivery of high-quality outcomes. Showing passion, persistence and resilience in seeking creative solutions to strive for continuous improvement and excellence.
- **Integrity**
  Acting always with the interests of children and young people at our heart, and with a consistent and uncompromising adherence to strong moral and ethical principles. Communicating with transparency and respect, creating a working environment based on trust and honesty.
- **Compassion**
  Recognising need in others and acting with positive intention to promote well-being and improve outcomes.

Providing Accessible Formats

If you are unable to use this document and require it in a different format please contact the Director of Safeguarding.

Contents

Linked Policies and Documents

- Keeping Children Safe in Education
- Teaching Online Safety in Schools
- WeST Child Protection and Safeguarding Policy
- WeST Data Protection Policy
- WeST Staff Code of Conduct
- WeST guidance on use of social media

Introduction

In line with the DFE guidance[1] on teaching online safety in schools. Hele's School recognises that the use of technology has become a significant component of many safeguarding issues. In cases of child sexual exploitation, radicalisation, and sexual predation technology often provides the platform that facilitates harm. An effective approach to online safety empowers a school to protect and educate the whole school community in their use of technology and establishes mechanisms to identify and intervene in and escalate any incident where appropriate. Hele's Schools's online Safety Policy outlines how this is achieved.

Hele's School recognises that the The breadth of issues classified within online safety is considerable and ever evolving, but can be categorised into four areas of risk:

- **content**: being exposed to illegal, inappropriate, or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, and extremism.
- **contact**: being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.
- **conduct**: online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g. consensual and nonconsensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying

[1] https://www.gov.uk/government/publications/teaching-onlinonline safety-in-schools/teaching-onlinonline safety-in-schools

- **commerce**: risks such as online gambling, inappropriate advertising, phishing and or financial scams. If you feel your pupils, students or staff are at risk, please report it to the Anti-Phishing Working Group (https://apwg.org/).

Policy Rationale

Online safety comprises all aspects relating to children and young people and their safe use of the internet, mobile phones, and other technologies, both in and out of school. It highlights the need to educate children, young people, parents, staff, and all members of the school community about the benefits, risks and responsibilities of using information technology and provides safeguards and awareness for users to enable them to control their online experiences.

The internet is an open communications channel, available to all. Applications such as the web, e-mail, blogs, and social networking all transmit information over the fibres of the internet to many locations in the world at low cost. Anyone can send messages, discuss ideas, and publish material with little restriction. These features of the internet make it an invaluable resource used by millions of people every day. Much of the material on the internet is published for an adult audience and some is unsuitable for pupils. Pupils must also learn that publishing personal information could compromise their security. This policy applies to all members of the Hele's School community (including staff, pupils, volunteers, parents / carers, visitors, and community users) who have access to and are users of school ICT systems, both in and out of school.

Headteachers are empowered, to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and may impose disciplinary penalties for inappropriate behaviour, as laid out in the school's behavoiur policy[2]. This is pertinent to incidents of cyber-bullying, or other online safety incidents covered by this policy, which may take place out of school, but is linked to membership of the school.

The school will deal with such incidents within this policy and associated behaviour and antibullying policies and will, where known, inform parents / carers of incidents of inappropriate online safety behaviour that take place out of school.

Policy Statements

Education – Pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in online safety is therefore an essential part of the school's online safety provision. Children and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience. Online safety education will be provided in the following ways:

- A planned online safety education will be provided as part of Computer Science lessons, the assembly programme and PD curriculum. This will cover both the use of ICT and new technologies in school and outside school.
- Pupils should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.
- Pupils will be helped to understand the need for the Pupil ICT Code of Conduct and encouraged to adopt safe and responsible use of ICT, the internet, and mobile devices both within and outside school.
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- Staff should act as good role models in their use of ICT, the internet, and mobile devices.

[2] https://www.gov.uk/government/publications/behaviour-in-schools--2

Education – Parents and Carers
Many parents and carers have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring and regulation of the children's online experiences. Parents often either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it.

The school will therefore seek to provide information and awareness to parents and carers through:

- Letters, newsletters, and the school website.
- Online safety communications via InTouch.

Training – Staff
It is essential that all staff receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- Online safety training will be provided annually to all staff as part of the school's ongoing safeguarding training offer.
- All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the school Online Safety Policy and WeST Staff Code of Conduct.
- This Online Safety Policy and its updates will be presented to and discussed by staff in staff meetings.
- The Online Safety Officer/DSL will provide advice, guidance and training to individuals as required.

Training – Governance
Those in governance across WeST (known as Trustees and HAB Members) should take part in online safety training and awareness sessions, with importance for those who are members of any subcommittee, group involved in ICT, online safety, health and safety and child protection. This may be offered in several ways:

- Participation in school training events.
- Attendance at training provided by the National Governors Association, WeST or other relevant organisation.

Roles and Responsibilities

The following section outlines the roles and responsibilities for online safety of individuals and groups within the school:

Trustees
Trustees are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. Monitoring will be carried out by the Education Standards Panel and Hub Advisory Boards (HABs) who will receive regular information about online safety incidents and monitoring reports via the Director of Safeguarding.

Those in governance can fulfil this responsibility in the following ways:

- Approving this policy and strategy and subsequently review its effectiveness, e.g. by asking the questions in the helpful document from the UK Council for Child Internet Safety (UKCIS) Online safety in schools and colleges: Questions from the Governing Board [3]
- "Ensuring an appropriate **senior member** of staff, from the school or college leadership team, is appointed to the role of DSL [with] **lead responsibility** for safeguarding and child protection (including online safety) [with] the appropriate status and authority [and] time, funding, training, resources and support…"

[3] https://www.gov.uk/government/publications/online-safety-in-schools-and-colleges-questions-from-the-governing-board

- Supporting the school in encouraging parents and the wider community to become engaged in online safety activities
- Having regular strategic reviews with the online safety co-ordinator / DSL and incorporate online safety into standing discussions of safeguarding at governance meetings
- Where the online safety coordinator is not the named DSL or deputy DSL, ensuring that there is regular review and open communication between these roles and that the DSL's clear overarching responsibility for online safety is not compromised
- Working with the WeST DPO (alongside WeST's commissioned data protection service providers), DSL and Headteacher to ensure a GDPR-compliant framework for storing data, but helping to ensure that child protection is always put first and data-protection processes support careful and legal sharing of information
- Checking all school staff have read the appropriate sections of the latest version of Keeping Children Safe in Education[4]

Headteacher and Senior Leaders

The Headteacher is responsible for ensuring the safety (including online safety) of members of the school community, though the day-to-day responsibility for online safety will be delegated to the online safety officer/DSL.

The Headteacher / Senior Leaders are responsible for ensuring that the online safety officer/DSL and other relevant staff receive suitable CPD to enable them to carry out their online safety roles and to train other colleagues, as relevant.

The Headteacher / Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role.

The Headteacher and online safety officer/DSL should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff (please also see the WeST Disciplinary Policy and Procedure).

The Headteacher should:

- Foster a culture of safeguarding where online safety is fully integrated into whole-school safeguarding
- Oversee the activities of the DSL and ensure that the DSL responsibilities listed in the section below are being followed and fully supported
- Ensure that policies and procedures are followed by all staff
- Undertake training in offline and online safeguarding, in accordance with statutory guidance and relevant Local Safeguarding Partnerships
- Liaise with the DSL on all online safety issues which might arise and receive regular updates on school issues and broader policy and practice information
- Take overall responsibility for data management and information security ensuring the school's provision follows best practice in information handling; work with the DPO, DSL and those in governance to ensure a GDPR-compliant framework for storing data, but helping to ensure that child protection is always put first and data-protection processes support careful and legal sharing of information

[4] https://www.gov.uk/government/publications/keeping-children-safe-in-education--2

- Ensure the school implements and makes effective use of appropriate ICT systems and services including school-safe filtering and monitoring, protected email systems and that all technology including cloud systems are implemented according to child-safety first principles
- Be responsible for ensuring that all staff receive suitable training to carry out their safeguarding and online safety roles
- Understand and make all staff aware of procedures to be followed in the event of a serious online safeguarding incident
- Ensure suitable risk assessments are undertaken so the curriculum meets needs of pupils, including risk of children being radicalised
- Ensure that there is a system in place to monitor and support staff (e.g., network manager) who carry out internal technical online safety procedures
- Ensure those in governance are regularly updated on the nature and effectiveness of the school's arrangements for online safety
- Ensure the school website meets statutory requirements

Online safety officer/DSL
Takes day-to-day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies / documents. The role includes:

- Ensuring that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- Providing training and advice for staff.
- Liaising with the Local Authority, when needed.
- Liaising with school ICT technical staff. Along with administration / marketing / other key support staff
- Receiving reports of serious online safety incidents and uses this to inform future online safety developments.
- Reviewing incident and filtering logs, when highlighted by the Network Manager.
- Reporting regularly to Senior Leadership Team.
- Regularly testing the schools fltering systems using the www.testfiltering.com website and keeping records of the test results

Network Manager
The Network Manager is responsible for ensuring:

- That the school's ICT infrastructure is secure and is not open to misuse or malicious attack.
- That users may only access the school's networks through a properly enforced password protection policy, in which passwords are regularly changed.
- The school's filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person.
- That they keep up to date with online safety technical information to effectively carry out their online safety role and to inform and update others as relevant.
- That the use of the network / remote access / email is regularly monitored in order that any misuse or attempted misuse can be reported to the Headteacher for investigation.
- That monitoring software / systems are implemented and updated as agreed in school policies.

Teaching and Support Staff
Teaching and support staff are responsible for ensuring that:

- They have an up-to-date awareness of online safety matters and of the current school Online Safety Policy and practices.
- They have read, understood, and signed the Staff Code of Conduct.
- They report any suspected misuse or problem to the online safety officer/DSL/Headteacher for investigation and action.
- Digital communications[5] with pupils or other stakeholders are on a professional level and only carried out using official school systems.
- Online safety issues are embedded in all aspects of the curriculum and other school activities.
- Pupils understand and follow the school Online Safety Policy.
- Pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- They monitor ICT activity in lessons, extra-curricular and extended school activities.
- They are aware of online safety issues related to the use of mobile phones, media devices, cameras, and handheld devices and that they monitor their use and implement current school policies about these devices.
- In lessons where internet use is pre-planned pupils 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.

Designated Safeguarding Lead & Deputy Safeguarding Leads
The DSL and Deputy DSLs should be trained in online safety issues and be aware of the potential for serious child protection issues to arise from:

- Sharing of personal data.
- Access to illegal / inappropriate materials.
- Inappropriate on-line contact with adults / strangers.
- Youth produced sexual imagery (also known as 'nudes', 'semi nudes' or 'sexting')
- Potential or actual incidents of grooming / child sexual exploitation.
- Cyber-bullying.

It is important to emphasise that these are child protection issues, not technical issues, simply that the technology provides additional means for child protection issues to develop.

Pupils
Pupils are responsible:

- For using the school ICT systems in accordance with the pupil code of conduct for ICT, which they will be expected to sign before being given access to school systems.
- Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- Understanding the importance of reporting abuse, misuse, or access to inappropriate and/or extremist materials and know how to do so.
- Will be expected to know and understand school policies on the use of mobile phones (dependent on their school setting), digital cameras, and handheld devices. They should also know and understand school policies on the taking / use of images and on cyber-bullying.
- Should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's Online safety Policy covers their actions out of school, if related to their membership of the school.

[5] This includes **all** forms of digital communication such as, but not limited, to the following: email, Teams messages, ClassCharts messaging and Class DoJo Messaging

Curriculum

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages in the use of ICT across the curriculum.

In lessons where internet use is pre-planned, it is best practice that pupils 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.

Where pupils can freely search the internet, e.g., using search engines, staff should be vigilant in monitoring the content of the websites the young people visit.

It is accepted that from time to time, for good educational reasons, pupils may need to research topics (e.g., racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Network Manager temporarily remove those sites from the filtered list for the period of study. Any request to do so should be auditable, with clear reasons for the need.

Pupils should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.

Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.

Data Protection

Personal data will be recorded, processed, transferred, and made available according to the principles set out in UK GDPR legislation which states that personal data must be:

- Fairly,lawfully and transparentlyprocessed.
- Collected for specified, explicit and legitimate purposes.
- Adequate, relevant, and limited to what is necessary in relation to the stated purpose. .
- Accurate and kept up to date.
- Kept no longer than is necessary for the purpose stated or required by legislation.
- Processed in manner that ensures appropriate security.

The data controller shall be responsible for, and be able to demonstrate compliance with, the principles set out in legislation. Staff must ensure that:

- At all times they take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Personal data is only stored with secure password protected school systems or online providers.
- They are properly “logged-off” at the end of any session.
- They use appropriate systems to ensure the security of personal data if asked to transfer information between schools or to external organisations.

For full guidance regarding data protection requirements please refer to the WeST Data Protection Policy at: Westcountry Schools Trust - Our Policies (weststs.org.uk)

Communication

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

- The official school email service may be regarded as safe and secure and is monitored. Staff and pupils should therefore use the school email service to communicate with others when in school, or on school systems (e.g. by remote access).
- Users need to be aware that email communications may be monitored.
- All staff must adhere to the email protocol.
- Users must immediately report, to the Headteacher, online safety officer/DSL or Network Manager (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 pupils or parents / carers must be professional in tone and content. These communications should only take place on official (monitored) school systems[6]. Personal email addresses, text messaging or public chat / social networking programmes (e.g. What's App) must not be used for these communications.
- Personal information should not be posted on the school website and only official email addresses should be used for communication.

Social Media - Protecting Professional Identity

With an increase in use of all types of social media for professional and personal purposes a policy that sets out clear guidance for staff to manage risk and behaviour online is essential. Core messages should include the protection of pupils, the school and the individual when publishing any material online. Expectations for teachers' professional conduct are set out in the 'Teachers Standards'[7].

All schools, academies and local authorities have a duty of care to provide a safe learning environment for pupils and staff. Schools/academies and local authorities could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, cyberbully, discriminate on the grounds of sex, race, or disability or who defame a third party may render Hele's School liable to the injured party.

Reasonable steps to prevent predictable harm must be in place. The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff, and the school through limiting access to personal information:

- Training to include acceptable use; social media risks; checking of settings; data protection; reporting issues.
- Clear reporting guidance, including responsibilities, procedures, and sanctions.
- Risk assessment, including legal risk.

School staff should ensure that:

- No reference should be made in social media to pupils, parents/carers, or school staff.
- They do not engage in online discussion on personal matters relating to members of the school community.
- Personal opinions should not be attributed to the school.
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

Unsuitable / inappropriate activities

Some internet activity e.g., accessing child abuse images or distributing racist or extremist material is illegal and is obviously banned from Hele's School and all other technical systems.

[6] Such systems include email, Teams messages, ClassCharts messaging and Class DoJo messaging.

[7] https://www.gov.uk/government/publications/teachers-standards

Other activities e.g., cyber-bullying is also banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would be inappropriate in a school context, either because of the age of the users or the nature of those activities.

The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in school or outside school when using school equipment or systems. The school policy restricts usage as outlined on the next page.

User Actions

		Acceptable	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	**Child sexual abuse images –The making, production, or distribution of indecent images of children. Contrary to The Protection of Children Act 1978**				X
	Grooming, incitement, arrangement, or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.				X
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008				X
	Criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986				X
	Pornography			X	
	Promotion of any kind of extremist viewpoints and discrimination			X	
	Threatening behaviour, including promotion of physical violence or mental harm			X	
	Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute			X	
Using school systems to run a private business				X	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school / academy				X	
Infringing copyright				X	
Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords)				X	
Creating or propagating computer viruses or other harmful files				X	
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)				X	
On-line gaming (educational)		X			
On-line gaming (non-educational)				X	
On-line gambling				X	
On-line shopping / commerce			X		
File sharing			X		
Use of social media			X		

Use of messaging apps		X		
Use of video broadcasting e.g. YouTube		X		

Technical – infrastructure/equipment, filtering and monitoring

Keeping Children Safe in Education[8] obliges schools to "*ensure appropriate filters and appropriate monitoring systems are in place [and] not be able to access harmful or inappropriate material [but at the same time] be careful that "over blocking" does not lead to unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding*."

WeST is responsible for ensuring:

- School technical systems will be managed in ways that ensure that the school meets recommended technical requirements.
- There will be regular reviews and audits of the safety and security of school technical systems.
- Servers, wireless systems, and cabling must be securely located and physical access restricted.
- All users will have clearly defined access rights to school technical systems and devices.
- Users in primary (at KS2 and above) MAY be provided with a username and secure password. Users are responsible for the security of their username and password and will be required to change their password every year. (If in any given period schools choose to use group or class log-ons, schools make sure that staff are aware of the associated risks).
- The 'master/administrator' passwords for the school ICT system, used by the Network Manager must also be available to the Headteacher or other nominated senior leader and kept in a secure place (e.g. school safe).
- WeST is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations (Inadequate licencing could cause the school to breach the Copyright Act which could result in fines or unexpected licensing costs).
- Internet access is filtered for all users by Smoothwall through WeST IT servuces. Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated, and internet use is logged and regularly monitored. There is a clear process in place to deal with requests for filtering changes.
- Internet filtering should ensure that children are safe from terrorist and extremist material when accessing the internet[9].
- The school has provided enhanced/differentiated user-level filtering (allowing different filtering levels for different ages/stages and different groups of users – staff/pupils/pupils etc).
- School technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement.
- An appropriate system is in place for users to report any actual/potential technical incident/ security breach to the relevant person, as agreed. At Hele's School school this is Mr Gavin Main, Network Manager. In the absence of the Network Manager, responsibility should fall to the Senior IT Technician, Mr David Lynas. If no technical staff are available, the DSL or Principal should be immediately informed to escalate the breach and liaise with WeST central IT services or external support contractors (currently Judicium at WeST).
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts which might threaten the security of the

[8] https://www.gov.uk/government/publications/keeping-children-safe-in-education--2

[9] NB: additional duties for schools/academies under the Counter Terrorism and Securities Act 2015 which requires schools/academies to ensure that children are safe from terrorist and extremist material on the internet.

school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up-to-date virus software.

- An agreed policy is in place for the provision of temporary access of "guests" (e.g., trainee teachers, supply teachers, visitors) onto the school systems.
- An agreed policy is in place regarding the extent of personal use that users (staff/pupils/pupils/community users) and their family members are allowed on school devices that may be used out of school.
- An agreed policy is in place that allows staff to/forbids staff from downloading executable files and installing programmes on school devices.
- An agreed policy is in place regarding the use of removable media (e.g., memory sticks/CDs/ DVDs) by users on school devices. Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

Remote Learning: Staff guidance for live lessons on MS Teams

Hele's School uses Microsoft Teams as a normal way of working and may use it to support pupils' online learning during periods of school 'closure', such as those that happened during the Covid-19 pandemic. In such circumstances pupils benefit greatly from live lessons as teachers can cover greater subject content and give specific feedback on how to improve. Safeguarding is always our key priority, and the following protocols are in place for staff, parents, and pupils so that we can maximize pupil learning.

Attendance, Behaviour and Safeguarding

- Attendance is compulsory in all remote live lessons. Teachers should take the register and non-attendance will be followed up as per normal school procedures.
- For safeguarding purposes, the lesson will be recorded. This will not be published or shared and will be stored in line with data protection requirements. You will receive an email of the recording, please retain it for 6 months.
- The pupil code of conduct specifies that behaviour should be committed, respectful and safe. Pupils who exceed our expectations should be rewarded and those who fall short should be sanctioned.

Before the lesson:

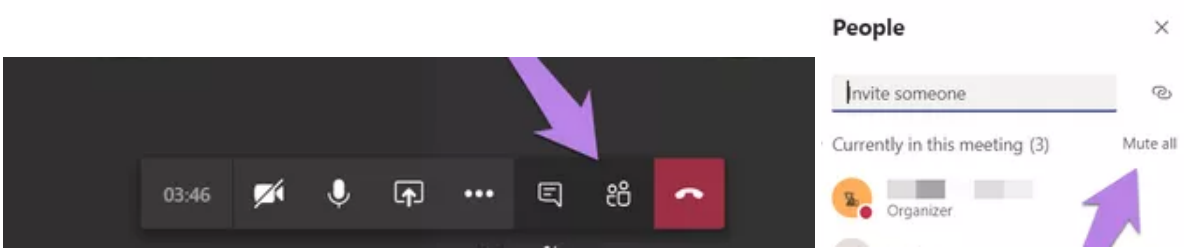
- Staff should ensure that all classes are activated on Teams and that security settings have checked.

Venue and equipment

- Staff are encouraged to use their timetabled classroom for the lesson.
- All classrooms have a visualiser with a camera and microphone. Once you open the Teams meeting, before others join, adjust the visualiser to ensure your face is visible, and place it in front of you.
- Staff should access MS Teams through the start menu on the desktop **but** Office.com is available if necessary.

Lesson Start:

- Live, remote lessons should start 5 minutes after the formal start time of the lesson, to ensure teachers have time to move between classrooms and set up.
- Ensure that any external hardware required, e.g. speakers, has been activated.
- The teacher should record the lesson and pupils will automatically be alerted to this.
- The lesson should begin with pupils' cameras and microphones on for the introduction/welcome.
- For safeguarding purposes, the register should be completed within the first 10 minutes.
- After this, pupils should be asked to turn their cameras and microphones off. Teachers can mute all participants:



To end the lesson

- At the end of a Teams call, to stop pupils re-joining a Teams call without the teacher there, **teachers must click End Meeting, not the classic 'hang up' button.**
- Staff should raise any concerns they may have through the normal channels of communication with colleagues.

Online safety incident procedures

Out-of-school cyber-bullying incident

1. Head of Year to investigate incident.
2. Pupils involved to be spoken to.
3. Parents informed.
4. Appropriate sanctions issued.
5. SLT link to provide support.

In-school cyber-bullying incident (involving school network or mobile devices)

1. Head of Year to investigate incident.
2. Head of Year to contact Network Manager to have network access removed.
3. Parents informed.
4. Appropriate sanctions issued.
5. SLT link to provide support.

Accessing another person's network account without permission

1. If the incident happens within a lesson the responsibility for taking action lies with the subject teacher.
2. If the incident occurs outside of lesson time the Head of Year will take responsibility.
3. In both circumstances the Network Manager should be contacted, and network access removed for a fixed period.
4. Parents to be informed.

Accessing inappropriate/illegal/extremist material or bringing such material into school

1. If this involves the use of the school network, please contact the Network Manager immediately to ensure the user account is frozen to avoid deletion.
2. Referral to the appropriate Head of Year who will then investigate.
3. Consult with DSL and appropriate agencies, when required (especially for illegal or extremist materials).
4. Appropriate sanctions issued and network access removed for a fixed period.
5. Parents to be informed.
6. Pastoral team to work with pupil(s) so that they realise that accessing such material is not appropriate. In the event of several online safety incidents involving the same pupil(s) then referral to the online safety officer/DSL is appropriate.

On-line child protection / extremism / radicalisation concerns

1. Immediate referral to a Designated Safeguarding Lead in-line with safeguarding procedures.
2. DSL to coordinate response including possible police and social services involvement.

Appendix 1a: Hele's School Pupil Code of Conduct for ICT (Secondary)

I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users.

For my own personal safety:

- I understand that the school will monitor my use of the ICT systems, email, and other digital communications.
- I will not share my username and password, nor will I try to use any other person's username and password.
- I will be aware of the danger of talking to strangers when I am communicating online.
- I will not disclose or share personal information about myself or others when online.
- If I arrange to meet people off-line that I have communicated with on-line, I will inform my parents, do so in a public place and take an adult with me.
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.

I understand that everyone has equal rights to use technology as a resource and:
I understand that the school ICT systems are intended for educational use and that I will not use the systems for personal or recreational use unless I have permission from a member of staff to do so.

- I will not try (unless I have permission from a member of staff) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not use the school ICT systems for on-line gaming, on-line gambling, internet shopping, file sharing, or video broadcasting (e.g. YouTube)
- I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.
- I will be polite and responsible when I communicate with others, I will not use strong, aggressive, or inappropriate language and I appreciate that others may have different opinions.
- I will not take or distribute images of anyone without their permission.

I recognise that the school has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the smooth running of the school:

- I will only use my personal handheld / external devices (mobile phones / USB devices etc) in school if I have permission from a member of staff. I understand that, if I do use my own devices in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment.
- I understand the risks and will not try to upload, download, or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will immediately report any damage or faults involving equipment or software; however, this may have happened.
- I will not open any attachments to emails, unless I know and trust the person / organisation who sent the email, due to the risk of the attachment containing viruses or other harmful programmes.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings.
- I will not use chat and social networking sites at any time in school.

When using the internet for research or recreation, I recognise that:

- I should ensure that I have permission to use the original work of others in my own work.
- Where work is protected by copyright, I will not try to download copies (including music and videos).
- When I am using the internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.

I understand that I am responsible for my actions, both in and out of school:

- I understand that the school also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school where they involve my membership of the school community (examples would be cyber-bullying, use of images or personal information).
- I understand that if I fail to comply with this Code of Conduct, I will be subject to disciplinary action. This may include loss of access to the school network / internet, detentions, suspension, contact with parents and in the event of illegal activities involvement of the police.

Pupils

Please complete the agreement form on the last page to show that you have read, understood, and agree to the rules included in the Pupil Code of Conduct for ICT.

Parents

Please complete the agreement form on the next page to show that you have read, understood the rules included in the Pupil Code of Conduct for ICT.

Please retain the above Code of Conduct for reference – Only the agreement forms need to be returned to the school.

Appendix 3: Pupil Code of Conduct Agreement Form

Please complete the sections below to show that you have read, understood and agree to the rules included in the Code of Conduct.

If you do not sign and return this agreement, access to the school ICT systems will be removed.

I have read and understand the above and agree to follow these guidelines when:

- I use the school ICT systems and equipment (both in and out of school)
- I use my own equipment in school (when allowed) e.g., iPads, tablets, laptops, cameras etc…
- I use my own equipment out of school in a way that is related to me being a member of this school e.g., communicating with other members of the school, accessing school email, the intranet, website etc…

Signature……

Print name……..

Tutor group…….

Year group……..

Date…….

POLICY HISTORY

Policy Date	Summary of changes	Contact / Responsibility for Policy	Version/ Implementation Date	Review Date
March 2023	First version of this aligned policy for use across WeST schools, with local variation	Director of Inclusion	March 2025	March 2025
March 2025	• Addition of 4th C for Commerce as broad risks outlined in KCSiE. • Addition of www.testfiltering.com tests to DSL responsibilties (was in place previously in schools but not in policy • Clarified that proessional standards apply to all forms of digital messaging, i.e. not just email but also Teams messages etc. • Simplification of instructions to staff around use of Teams for remote lessons (based on increased levels of staff confidence)	Director of Safeguarding	March 2025	March 2027