•

Online Safety Policy

Policy Tracker – Responsibility for monitoring this policy: Trust IT Manager (Reviewed annually – date of next review Autumn 25)			
Date of review	**Reviewed by**	**Role**	**Date approved**
July 2020	**Claire Johnson**	**Deputy Headteacher**	**July 2020**
January 2021 (COVID amendments)	**Rebecca Cox**	**Director of School Improvement**	**January 2021**
July 2021	**Sue Harris**	**Trust IT Manager**	**Spring 2021**
September 2021	**Jeannette Mackinney**	**CEO**	**Updated in line with KCSIE**
February 2022 (Online Safety Committee review)	**Sue Harris**	**Trust IT Manager**	**May 2022**
March 2022 (Heads review and change of monitoring software)	**Sue Harris**	**Trust IT Manager**	**May 2022**
October 2022 (IT Leads and TIM Review)	**Sue Harris**	**Trust IT Manager**	**November 2022**
Sept 23 Review KCSIE (All Stakeholders Review)	**Sue Harris**	**Trust IT Manager**	**November 2023**

•

January 2024 Review (IT Leaders and TIM review)	**Sue Harris**	**Trust IT Manager**	**February 2024**
September 2024 All Stakeholders Review	**Sue Harris**	**Trust IT Manager**	**DRAFT FOR APPROVAL C & S Sept 24**

Contents

Development/Monitoring/Review of this Policy

This online safety policy has been developed by Director of Education (DOE) Trust IT Manager (TIM) and in consultation with the following:

- Executive Headteachers, Headteachers and senior leaders
- CEOP ambassador
- Staff – including teachers, support staff, technical staff
- Governors/Board
- Parents and carers

•

Consultation with the whole school community has taken place through a range of formal and informal meetings.

Schedule for Development/Monitoring/Review

This online safety policy was approved by the Curriculum and Standards Committee on:	***02/09/2024***
The implementation of this online safety policy will be monitored by the:	*Governors, DOE, TIM, EHT, HT, Computing Leads and technicians*
Monitoring will take place at regular intervals:	*Annually*
The Trust School improvement committee will receive a report on the implementation of the online safety policy generated by the monitoring group (which will include anonymous details of online safety incidents) at regular intervals:	*Annually*
The online safety policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place. The next anticipated review date will be: **September 25**	*Annually*
Should serious online safety incidents take place, the following external persons/agencies should be informed:	*LA Safeguarding Team, Senior officers, LADO, Police*

The school will monitor the impact of the policy using:

- Logs of reported incidents via Smoothwall Monitoring software (for monitoring) and MAT level overview with RM SafetyNet (for filtering)
- Monitoring logs of internet activity via Smoothwall Monitoring and RM SafetyNet software
- CPOMS – where logs of incidents relating to safety are stored.
- CPOMS and Smoothwall Monitoring integration - is used for monitoring child protection and a range of pastoral and welfare issues. Schools can see incidents relating to the student, with an indication that this came from Smoothwall Monitoring, when it was raised, the risk category and risk level. This can be reviewed, the incident can be attached to a student or deleted.
- RM SafetyNet By default, illegal websites are blocked by RM SafetyNet based on input from the Internet Watch Foundation, the Home Office, the Counter Terrorist list and security intelligence, including radicalisation content. The technology safeguards devices brought into school when they're connected to the network. Filtering preferences adjust access for different users.
- Alerts can be set up to notify the school of attempted access to harmful or sensitive content, highlighting any noncompliant browsing activity. The product is cloud-based, no additional hardware is required on site and the system will automatically update.
- Internal monitoring data for network activity and activity of wireless devices such as Chromebooks ○ Surveys/questionnaires of
    - ○ Pupils ○ parents/carer
    - s ○ staff

Scope of the Policy

This policy applies to all members of the Trust community (including staff, pupils, volunteers, parents/carers, visitors, community users) who have access to and are users of sites digital technology systems, both in and out of the school.

The Education and Inspections Act 2006 empowers Headteachers/Principals to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of online-bullying or other online safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data (see HVT Deletion of Data policy). In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

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

The school will ensure as soon as children's issues emerge, in school or online, prompt action is taken to resolve these.

This policy has due regard to all relevant legislation and guidance including, but not limited to, the following:

- Voyeurism (Offences) Act 2019
- The UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018

-
- DfE (2023) 'Filtering and monitoring standards for schools and colleges'
- DfE (2021) 'Harmful online challenges and online hoaxes'
- DfE (2023) 'Keeping children safe in education 2023'
- DfE (2023) 'Teaching online safety in school'
- DfE (2022) 'Searching, screening and confiscation'
- DfE (2023) 'Generative artificial intelligence in education'
- Department for Digital, Culture, Media and Sport and UK Council for Internet Safety (2020) 'Sharing nudes and seminudes: advice for education settings working with children and young people'
- UK Council for Child Internet Safety (2020) 'Education for a Connected World – 2020 edition'

Areas of online safety risk: Cybercrime referral

- Content: being exposed to illegal, inappropriate or harmful content such as pornography, fake news, misogyny, selfharm, suicide, radicalisation and extremism
- Contact: being subjected to harmful online interaction with other users such as child-on-child pressure and adults posing as children or young adults to groom or exploit children
- Conduct: personal online behaviour that increases the likelihood of, or causes, harm such as making, sending and receiving explicit images, sharing other explicit images and online bullying
- Commerce: risks such as online gambling, inappropriate advertising, phishing or financial scams.
- Cybercrime is criminal activity committed using computers and/or the internet. It is broadly categorised as either 'cyber-enabled' (crimes that can happen offline but are enabled at scale and at speed online) or 'cyber dependent' (crimes that can be committed only by using a computer). Cyber-dependent crimes include:
- unauthorised access to computers (illegal 'hacking'), for example accessing a school's computer network to look for test paper answers or change grades awarded
- 'Denial of Service' (Dos or DDoS) attacks or 'booting'. These are attempts to make a computer, network or website unavailable by overwhelming it with internet traffic from multiple sources, and,
- making, supplying or obtaining malware (malicious software) such as viruses, spyware, ransomware, botnets and Remote Access Trojans with the intent to commit further offence, including those above.

Cyber-enabled: these crimes can be carried out offline; however, are made easier and can be conducted at higher scales and speeds online, e.g. fraud, purchasing and selling of illegal drugs, and sexual abuse and exploitation.

Children with particular skills and interest in computing and technology may inadvertently or deliberately stray into cyberdependent crime. If there are concerns about a child in this area, the designated safeguarding lead (or deputy), should consider referring into the Cyber Choices programme. This is a nationwide police programme supported by the Home Office and led by the National Crime Agency, working with regional and local policing. It aims to intervene where young people are at risk of committing, or being drawn into, low-level cyber-dependent offences and divert them to a more positive use of their skills and interests

Cyber Choices does not currently cover 'cyber-enabled' crime such as fraud, purchasing of illegal drugs online and child sexual abuse and exploitation, nor other areas of concern such as online bullying or general on-line safety. Additional advice can be found at: http://www.cyberchoices.uk/, https://www.ncsc.gov.uk/, https://www.nspcc.org.uk/keeping-childrensafe/reporting-abuse/what-if-suspect-abuse/

Cyberbullying

Cyberbullying can include, but is not limited to, the following:

- Threatening, intimidating or upsetting text messages
- Threatening or embarrassing pictures and video clips sent via mobile phone cameras
- Silent or abusive phone calls or using the victim's phone to harass others, to make them think the victim is responsible
- Threatening or bullying emails, possibly sent using a pseudonym or someone else's name
- Unpleasant messages sent via instant messaging
- Unpleasant or defamatory information posted to blogs, personal websites and social networking sites, e.g. Facebook
- Abuse between young people in intimate relationships online i.e. teenage relationship abuse
- Discriminatory bullying online i.e. homophobia, racism, misogyny/misandry.

The school will be aware that certain pupils can be more at risk of abuse and/or bullying online, such as LGBTQ+ pupils and pupils with SEND.

Cyberbullying against pupils or staff is not tolerated under any circumstances. Incidents of cyberbullying are dealt with quickly and effectively wherever they occur in line with the Anti-bullying Policy.

Child-on-child sexual abuse and harassment

Pupils may also use the internet and technology as a vehicle for sexual abuse and harassment. Staff will understand that this abuse can occur both in and outside of school, off and online, and will remain aware that pupils are less likely to

•
report concerning online sexual behaviours, particularly if they are using websites that they know adults will consider to be inappropriate for their age.
The following are examples of online harmful sexual behaviour of which staff will be expected to be aware:
- Threatening, facilitating or encouraging sexual violence
- Upskirting, i.e. taking a picture underneath a person's clothing without consent and with the intention of viewing their genitals, breasts or buttocks
- Sexualised online bullying, e.g. sexual jokes or taunts
- Unwanted and unsolicited sexual comments and messages
- Consensual or non-consensual sharing of sexualised imagery
- Abuse between young people in intimate relationships online, i.e. teenage relationship abuse

All staff will be aware of and promote a zero-tolerance approach to sexually harassing or abusive behaviour, and any attempts to pass such behaviour off as trivial or harmless. Staff will be aware that allowing such behaviour could lead to a school culture that normalises abuse and leads to pupils becoming less likely to report such conduct.
Staff will be aware that creating, possessing, and distributing indecent imagery of other children, i.e. individuals under the age of 18, is a criminal offence, even where the imagery is created, possessed, and distributed with the permission of the child depicted, or by the child themselves.
The school will be aware that interactions between the victim of online harmful sexual behaviour and the alleged perpetrator(s) are likely to occur over social media following the initial report, as well as interactions with other pupils taking "sides", often leading to repeat harassment. The school will respond to these incidents in line with the Child-on-child Abuse Policy and the Social Media Policy.
The school will respond to all concerns regarding online child-on-child sexual abuse and harassment, regardless of whether the incident took place on the school premises or using school-owned equipment. Concerns regarding online child-on-child abuse will be reported to the DSL, who will investigate the matter in line with the Child-on-child Abuse Policy and the Child Protection and Safeguarding Policy.
Grooming and exploitation
Grooming is defined as the situation whereby an adult builds a relationship, trust and emotional connection with a child with the intention of manipulating, exploiting and/or abusing them.
Staff will be aware that grooming often takes place online and that pupils who are being groomed are commonly unlikely to report this behaviour for many reasons, e.g. the pupil may have been manipulated into feeling a strong bond with their groomer and may have feelings of loyalty, admiration, or love, as well as fear, distress and confusion.
Due to the fact pupils are less likely to report grooming than other online offences, it is particularly important that staff understand the indicators of this type of abuse. The DSL will ensure that online safety training covers online abuse, the importance of looking for signs of grooming, and what the signs of online grooming are, including:
- Being secretive about how they are spending their time online.
- Having an older boyfriend or girlfriend, usually one that does not attend the school and whom their close friends have not met.
- Having money or new possessions, e.g. clothes and technological devices, that they cannot or will not explain.

Child sexual exploitation (CSE) and child criminal exploitation (CCE)
Although CSE often involves physical sexual abuse or violence, online elements may be prevalent, e.g. sexual coercion and encouraging children to behave in sexually inappropriate ways through the internet. In some cases, a pupil may be groomed online to become involved in a wider network of exploitation, e.g. the production of child pornography or forced child prostitution and sexual trafficking.
CCE is a form of exploitation in which children are forced or manipulated into committing crimes for the benefit of their abuser, e.g. drug transporting, shoplifting and serious violence. While these crimes often take place in person, it is increasingly common for children to be groomed and manipulated into participating through the internet.
Where staff have any concerns about pupils with relation to CSE or CCE, they will bring these concerns to the DSL without delay, who will manage the situation in line with the Child Protection and Safeguarding Policy.
Radicalisation
Radicalisation is the process by which a person comes to support terrorism and extremist ideologies associated with terrorist groups. This process can occur through direct recruitment, e.g. individuals in extremist groups identifying, targeting and contacting young people with the intention of involving them in terrorist activity, or by exposure to violent ideological propaganda. Children who are targets for radicalisation are likely to be groomed by extremists online to the extent that they believe the extremist has their best interests at heart, making them more likely to adopt the same radical ideology.
Staff members will be aware of the factors which can place certain pupils at increased vulnerability to radicalisation, as outlined in the Prevent Duty Policy. Staff will be expected to exercise vigilance towards any pupils displaying indicators that they have been, or are being, radicalised.
Where staff have a concern about a pupil relating to radicalisation, they will report this to the DSL without delay, who will handle the situation in line with the Prevent Duty Policy.

Mental health

•

Staff will be aware that online activity both in and outside of school can have a substantial impact on a pupil's mental state, both positively and negatively. The DSL will ensure that training is available to help ensure that staff members understand popular social media sites and terminology, the ways in which social media and the internet in general can impact mental health, and the indicators that a pupil is suffering from challenges in their mental health. Concerns about the mental health of a pupil will be dealt with in line with the Social, Emotional and Mental Health (SEMH) Policy.

Online hoaxes and harmful online challenges

For the purposes of this policy, an "online hoax" is defined as a deliberate lie designed to seem truthful, normally one that is intended to scaremonger or to distress individuals who come across it, spread on online social media platforms.

For the purposes of this policy, "harmful online challenges" refers to challenges that are targeted at young people and generally involve users recording themselves participating in an online challenge, distributing the video through social media channels and daring others to do the same. Although many online challenges are harmless, an online challenge becomes harmful when it could potentially put the participant at risk of harm, either directly as a result of partaking in the challenge itself or indirectly as a result of the distribution of the video online – the latter will usually depend on the age of the pupil and the way in which they are depicted in the video.

Where staff suspect there may be a harmful online challenge or online hoax circulating amongst pupils in the school, they will report this to the DSL immediately.

The DSL will conduct a case-by-case assessment for any harmful online content brought to their attention, establishing the scale and nature of the possible risk to pupils, and whether the risk is one that is localised to the school or the local area, or whether it extends more widely across the country. Where the harmful content is prevalent mainly in the local area, the DSL will consult with the LA about whether quick local action can prevent the hoax or challenge from spreading more widely.

Prior to deciding how to respond to a harmful online challenge or hoax, the DSL and the headteacher will decide whether each proposed response is:

- In line with any advice received from a known, reliable source, e.g. the UK Safer Internet Centre, when fact-checking the risk of online challenges or hoaxes.
- Careful to avoid needlessly scaring or distressing pupils.
- Not inadvertently encouraging pupils to view the hoax or challenge where they would not have otherwise come across it, e.g. where content is explained to younger pupils but is almost exclusively being shared amongst older pupils.
- Proportional to the actual or perceived risk.
- Helpful to the pupils who are, or are perceived to be, at risk.
- Appropriate for the relevant pupils' age and developmental stage.
- Supportive.
- In line with the Child Protection and Safeguarding Policy.

Where the DSL's assessment finds an online challenge to be putting pupils at risk of harm, they will ensure that the challenge is directly addressed to the relevant pupils, e.g. those within a particular age range that is directly affected or individual pupils at risk where appropriate.

The DSL and headteacher will only implement a school-wide approach to highlighting potential harms of a hoax or challenge when the risk of needlessly increasing pupils' exposure to the risk is considered and mitigated as far as possible.

Roles and Responsibilities

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

Board of Directors

The Curriculum and Standards committee are responsible for the approval of the online safety policy and for reviewing the effectiveness of the policy. This will be carried out by the Curriculum and Standards Committee receiving regular information about online safety incidents and monitoring reports. A member of the Board has taken on the role of Online Safety Director as

•

it is part of the Child Protection/Safeguarding Governor role. As part of this process, governing bodies and proprietors should ensure their school or college has appropriate filtering and monitoring systems in place and regularly review their effectiveness. They should ensure that the leadership team and relevant staff have an awareness and understanding of the provisions in place and manage them effectively and know how to escalate concerns when identified. Governing bodies and proprietors should consider the number of and age range of their children, those who are potentially at greater risk of harm and how often they access the IT system along with the proportionality of costs versus safeguarding risks. The role of the Online Safety Director will include:

- receive communication from the TIM covering information around online safety management across the Trust
  receive minutes of meetings of the Online Safety Group
- monitor online safety incident logs via the TIM report
- monitor of filtering/change control logs via the TIM report
- reporting to Curriculum and standards committee • Check status of schools 360 Safe progress and awards.

Executive Headteacher, Heads and Senior Leaders

- The Executive Headteacher, Head has a duty of care 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 Lead*/Computing Leader
- The Executive Headteacher, Heads and (at least) another member of the Senior Leadership Team 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. (see flow chart on dealing with online safety incidents – included in a later section – "Responding to incidents of misuse" and relevant Trust disciplinary procedures).
- The Executive Headteacher, Heads and Senior Leaders are responsible for ensuring that the Online Safety Lead and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.
- The Executive Headteacher, Heads and 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. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- *The Senior Leadership Team will receive regular monitoring reports from the Online Safety Lead*/Computing Leader and the TIM. TIM liaises with IT Leads at least termly during the IT Leaders Online Safety Meetings, IT Leads to communicate outcome to SLT at least termly.
- All staff should receive appropriate safeguarding and child protection training (including online safety which, amongst other things, includes an understanding of the expectations, applicable roles and responsibilities in relation to filtering and monitoring.
- Staff should also undertake appropriate cyber security training provided by the school. (NSCS training/Boxphish).

Online Safety Lead (possibly working with your Computing Leader – ideally should have DSL status)

- leads the Online Safety work in school
- attends Trust Online Safety Group meetings
- takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies/documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- provides training and advice for staff
- liaises with the Trust about online safety issues via the TIM
- liaises with school technical staff – if relevant
- receives reports of online safety incidents and creates a log of incidents to inform future online safety developments which is logged on CPOMS and tagged as an e-safety incident,
- meets regularly with TIM to discuss current issues, review incident logs and filtering/change control logs
- attends relevant meetings of Online Safety Leads

-
- reports regularly to Senior Leadership Team
- undertake appropriate cyber security training provided by the school. (NSCS training/Boxphish).

Trust IT Manager (TIM) and Technical staff

Those with technical responsibilities are responsible for ensuring:

- that the school's technical infrastructure is secure and is not open to misuse or malicious attack
- that the school meets required online safety technical requirements and any online safety policy/guidance that may apply.
- that users may only access the networks and devices through a properly enforced password protection system
- the RM SafetyNet filtering system is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person (see appendix "Technical Security Policy")

  that they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant – including becoming a CEOP ambassador
- that the use of the networks/internet/digital technologies is regularly monitored in order that any misuse/attempted misuse can be reported to the Executive Headteacher, Heads, Senior Leaders, DSLs and Online Safety Lead for investigation/action/sanction
- that monitoring software/systems are implemented and updated as agreed in school policies • undertake appropriate cyber security training provided by the school. (NSCS training/Boxphish).

Teaching and Support Staff

Are responsible for ensuring that:

- they have an up to date awareness of online safety matters and in addition complete all Cyber Security training provided to them via Boxphish and NCSC and be aware of the current Trust Online Safety Policy and practices, at least on an annual basis
- they have read, understood and signed the staff acceptable use agreement
- they report any suspected misuse or problem to the Executive Headteacher/ Heads /Senior Leader/DSL/Online Safety Lead for investigation/action/sanctions which would be dependent on the level of severity, in line with the schools behaviour policy, and would also include education intervention around the incident cause. Possible sanctions for severe continued misuse may include, the removal of the network log on or access to IT devices being removed.
- all digital communications with pupils/parents/carers should be 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 activities
- pupils understand and follow the Online Safety Policy and acceptable use policies
- pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor the use of digital technologies, mobile devices, cameras, etc. in lessons and other school activities (where allowed) and implement current policies with regard to 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 Online Safety Lead

The designated safeguarding lead should take lead responsibility for safeguarding and child protection (including online safety and understanding the filtering and monitoring systems and processes in place).

RM (MSPs) have provided online seminars designed to support the DSL understand both the Filtering logs in RM SafetyNet and Monitoring results in Smoothwall monitor where incidents can be sent directly to CPOMs.

Undertake appropriate cyber security training provided by the school. (NSCS training/Boxphish).

•

Should be trained in online safety issues and be aware of the potential for serious child protection/safeguarding issues to arise from:

- sharing of personal data
- access to illegal/inappropriate materials
- inappropriate on-line contact with adults/strangers
- potential or actual incidents of grooming
- online-bullying

Trust Online Safety Group – (Consisting of Trust Computing Leaders)

The Online Safety Group provides a consultative group that has representation from the school community, with responsibility for issues regarding online safety and the monitoring the Online Safety Policy including the impact of initiatives. The group will also be responsible for regular reporting to the Online Safety Director via the Curriculum and standards committee. Online Safety Director is Mr M Simpson and will be invited to an IT Leads Online Safety Meeting.

Members of the Online Safety Group (or other relevant group) will assist the Online Safety Lead (or other relevant person, as above) with:

the production/review/monitoring of the school online safety policy/documents.

- the production/review/monitoring of the school filtering policy (if the school chooses to have one) and requests for filtering changes.
- mapping and reviewing the online safety/digital literacy curricular provision – ensuring relevance, breadth and progression
- monitoring network/internet/filtering/incident logs
- consulting stakeholders – including parents/carers and the pupils about the online safety provision • monitoring improvement actions identified through use of an approved national self-review tool 360 Safe.
- Report to the Headteacher of their school.
- Report to the Governors of their school.
- Respond to common issues within their school.

Pupils:

- are responsible for using the *school* digital technology systems in accordance with the student/pupil acceptable use agreement
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking/use of images and on online-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

Parents/carers

Parents/carers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website, social media and information about national/local online safety campaigns/literature. Parents and carers will be encouraged to support the school in promoting good online safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- access to parents' sections of the website/Google classroom and on-line student/pupil records

•

Community Users

Community Users who access school systems or programmes as part of the wider school provision will be expected to sign a Community User AUA before being provided with access to school systems. (A community users acceptable use agreement template can be found in the appendices.)

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/digital literacy 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.

In planning their online safety curriculum schools/academies may wish to refer to:

- DfE Teaching Online Safety in Schools
- Education for a Connected Word Framework
- SWGfL Project Evolve – online safety curriculum programme and resources

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

A planned online safety curriculum should be provided as part of Computing/PSHE/other lessons and should be regularly revisited, available resources National College/NOS and UKCCIS/ Curriculum programme of Study (eg Kapow) • Key online safety messages should be reinforced as part of a planned programme of assemblies

- 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
- Pupils should be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making**. N.B. additional duties for schools/academies under the Counter Terrorism and Securities Act 2015 which requires schools to ensure that children are safe from terrorist and extremist material on the internet –** NOTE: RM SafetyNet does filter material relating to extremism and radicalisation.
- Pupils should be helped to understand the need for the pupil acceptable use agreement and encouraged to adopt safe and responsible use both within and outside school.
- Staff should act as good role models in their use of digital technologies, the internet and mobile devices
- 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 are allowed to freely search the internet, 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 Technical Staff (or other relevant designated person) can 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.

Education – Parents/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/regulation of the children's online behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

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

-
- Curriculum activities
- Letters, newsletters, website, Learning Platform
- Parents/carers evenings/sessions
- High profile events/campaigns e.g. Safer Internet Day
- Specific Parent and Carers space on the school's website
- National Online Safety communications from the IT leaders to Parents in response to any specific school issues.

- Reference to the relevant web sites/publications e.g. swgfl.org.uk, www.saferinternet.org.uk/, http://www.childnet.com/parents-and-carers *(see appendix for further links/resources)*

Education – The Wider Community

The school will provide opportunities for local community groups/members of the community to gain from the school's online safety knowledge and experience. This may be offered through the following:

- Providing family learning courses in use of new digital technologies, digital literacy and online safety
- Online safety messages targeted towards grandparents and other relatives as well as parents.
- The school website will provide online safety information for the wider community
- Sharing their online safety expertise/good practice with other local schools
- Supporting community groups e.g. Early Years Settings, Childminders, youth/sports/voluntary groups to enhance their online safety provision
- Online Safety Self-Review Tool | 360 Early Years | 360 Early Years
- Online Safety Self-Review Tool for Groups | 360safe | 360safe (360groups.org.uk)

Education & Training – Staff/Volunteers

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:

- **A planned programme of formal online safety training using National Online Safety will be made available to staff. This will be regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out regularly**.
- **All new staff should receive online safety training as part of their induction programme, (this could be the online safety module using the Trust CPD packaged 'Flick' or via the school's own online safety training package they have purchased) ensuring that they fully understand the school online safety policy and acceptable use agreements.**
- The Online Safety Lead (or other nominated person) will receive regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisations. This includes 7 minute briefings on online dangers.
- This online safety policy and its updates will be presented to and discussed by staff in staff/team meetings/training sessions.
- The Online Safety Lead (or other nominated person such as a DSL) will provide advice/guidance/training to individuals as required.
- The Online Safety Lead will monitor and source training at least yearly.

Training – Governors/Directors

Governors/Directors should take part in online safety training/awareness sessions, with particular importance for those who are members of any group involved in technology/online safety/health and safety /safeguarding. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority/Trust/National Governors Association/or other relevant organisation such as through Governor Hub
- Participation in school training/information sessions for staff or parents
- National Online Safety online training.

Technical – infrastructure/equipment, filtering and monitoring

The school will be responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their online safety responsibilities:

- Filtering and Monitoring from DGFL our MSPs (Managed Service providers) ○ DGfL provides school-wide filtering and monitoring solutions using RM SafetyNet for web filtering and Smoothwall Monitor for on-device e-Safety monitoring and alerting. DGfL has setup all DGfL-provided network connections to require the use of RM SafetyNet web filtering with a base-level of filtering. DGfL has provided logins to school-nominated staff to access the system allowing the customisation of filtering policies and access to run reports. DGfL also offer a helpdesk service to assist schools with administering RM SafetyNet. DGfL has also provided training sessions to schools on how to make the best use of their web filtering system. DGfL has installed Smoothwall Monitor on all DGfL-managed devices which detects safeguarding concerns and alerts a school-nominated member of staff by email or telephone in the most serious cases. DGfL has offered Smoothwall Monitor training to all schools.
    - DGfL provides schools with access to RM SafetyNet and Smoothwall Monitor where they can view current policies and reports to allow schools to review if any changes are needed. The DGfL service desk can assist schools in making any changes needed. As part of DGfL's ITIL change control process, all changes are considered for their potential impact on e-Safety systems.

    - DGfL provides Smoothwall Monitor software for on-device monitoring. Any potential safeguarding issues detected by the software are reviewed by Smoothwall using both automated and human review and the school is notified in a timely fashion 24 hours a day. DGfL encourages schools to use named accounts for all staff and students so they can be easily identified in filtering and monitoring reports.

- All devices in DGfL schools are protected by RM SafetyNet filtering which is compliant with all Government restrictions. Filtering policies can be managed, (changes made), by DGfL and the individual school. This covers all devices either connected to the school network or wifi. Smoothwall Monitor is enabled on the following devices: DGfL-managed CC4 computers DGfL-managed Windows computers DGfL-managed Chromebooks, iPads managed by Intune MDM.

- Using UK Safer Internet Centre Filtering and Monitoring Checklist Register, spots checks are carried out across the Trust schools at the start of the new academic year by Trust IT Manager & Senior IT Technician (HVT IT Support). RM SafetyNet (filtering) is checked using "testingfiltering.com". Smoothwall Monitor (monitoring) is checked with a set of agreed search terms and then alerts the DSLs at the schools. Results send to Executive Heads, Heads and IT Leads.

- School technical systems will be managed in ways that ensure that the school meets recommended technical requirements
- There will be regular reviews and external 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.
- All users will be provided with a username and secure password by Trust IT Technicians who will keep an up to date record of users and their usernames. Users are responsible for the security of their username and password.
- The "master/administrator" passwords for the school systems, used by the Network Manager (or other person – usually the person who has access to the RM console) must also be available to the Executive Headteacher, Heads or other nominated senior leader and kept in a secure place (e.g. school safe)
- Trust IT leads and school Online safety leads are 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. Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the RM SafetyNet - Internet filtering designed for schools. Illegal websites are blocked by RM SafetyNet based on input from the Internet Watch Foundation (IWF), the Home Office, the Counter Terrorist list (CTIRU) and security intelligence, including radicalisation content. Some key features of RM SafetyNet are: ○ Adjustable access for different users ○ Protection for all devices
    - Instant reports when you need them via the web portal
    - Everyone accountable, everyone protected – All devices brought to school will be identifiable at user level ○ Useful alerts – Triggered if there is attempted access to particularly harmful or sensitive websites

There is a clear process in place to deal with requests for filtering changes. Any requests for change can be emailed directly to RM for filtering. You can also contact the Trust IT Manager or HVT Support Senior Technician. Internet filtering/monitoring should ensure that children are safe from terrorist and extremist material when accessing the internet. N.B. additional duties for schools under the Counter Terrorism and Securities Act 2015 which requires schools/ to ensure that children are safe from terrorist and extremist material on the internet. (see appendix for information on "appropriate filtering").

- In school - Smoothwall Monitoring and RM SafetyNet regularly monitor/filter and record the activity of users on the school technical systems and users are made aware of this in the acceptable use agreement. Hales Valley Trust uses Smoothwall Monitoring, Smoothwall Monitor is a real-time, digital monitoring solution that flags incidents as they happen. Monitoring both keystrokes and screen views, safeguarding staff are informed, through a variety of means, when users try to view or type harmful content. DSLs become aware of content that may indicate risk to a student such as cyberbullying, suicide, gang membership, violence, or an inappropriate use of school resources. Early identification of a risk, means early intervention and improved student outcomes. The system combines advanced intelligent detection software to identify threats others can't. Any changes required to Smoothwall Monitoring will be via the schools DSL (Designated Safeguarding Lead).

- In school - RM Safetynet by default, illegal websites are blocked by RM SafetyNet based on input from the Internet Watch Foundation (IWF), the Home Office, the Counter Terrorist list (CTIRU) and security intelligence, including radicalisation content. Our technology seamlessly safeguards devices brought into school when they're connected to the school internet too. You can easily add your own filtering preferences and adjust access for different users. Fulfilling responsibilities outlined in Keeping Children Safe in Education, The Prevent Duty and Ofsted's Common Inspection Framework whilst offering your pupils the freedom to learn from the biggest source of content in the world.
- *An appropriate system is in place* (to be described) *for users to report any actual/potential technical incident/security breach to the relevant person, as agreed). Any security breach should be reported as soon as noted within 72 hours to HR and Operations Manager who will provide advice on the breach and where necessary will advise the school to report to the Trusts named DPO (Your IG).. The HR and Operations Manager can inform the Trust IT Manager (TIM) and RM – Technical Account Manager, if required.*
- 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 school systems and data. These are tested regularly.
- The school infrastructure and individual devices are protected by up to date virus software.
- All school staff and visitors/supply staff have ID badges and must wear ID and scan into the buildings when on the school premises and scan out when they leave.
- Staff who have guardianship of school owned portable devices are required to sign them in and out of the school premises when scanning their ID badges to enter and leave the school building via the InVentry System. They are required to submit a signed Guardianship Form to the school before the items are removed from site.
- Staff and pupils have individual logs ons to the network.
- MFA (Multi-Factor-Authentication) is a requirement for all Teaching and Non-Teaching staff accessing RM Unify from outside the school buildings. (Authenticating apps maybe installed and used for authentication access **only** on staff personal mobiles when accessing from outside school).
- The access is adjusted for different network users.
- Where possible Mobile devices are stored in lockable areas on the school premises.
- When staff or visitors are using the school workstations they must log off or lock the station before moving away for any length of time – *this will be monitored via TIM no notice visits throughout the year.*
- Regular software updates are applied by the network providers (RM) to ensure the software has the latest security updates.
- Back up of systems are provided using Veeam and our network providers (RM) can restore the server and its date in a few hours should the worst happen.
- Our network providers (RM) have high end firewalls and best of breed adaptive antivirus.
- For the provision of temporary access of "guests" (e.g. trainee teachers, supply teachers, visitors) onto the school systems. Guest access is provided via Guest user log on. If guest access is required our network providers (RM) can provide the required access credentials. Guest users will have limited access to the schools systems. An agreed school policy is in place (to be described at school level)
- **School make an independent decision regarding the extent of personal use that users (staff/ pupils/community users) and their family members are allowed on school devices that may be used out of school. An agreed school policy is in place (to be described at school level)**
- RM systems forbid staff from downloading executable files and installing programmes on RM managed school devices. Schools must have their own in school procedures for manging this for non-RM managed devices.
- We do not use USB sticks in school. CDs and DVDs may be permitted with HVT Support authorisation. ***Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured***. (see School Personal Data Policy in the appendix for further detail). Where possible schools should insist that staff use a secure cloud based system i.e. One Drive and Teams to store and transfer documents.

Mobile Technologies (including BYOD/BYOT)

Mobile technology devices may be school owned/provided or personally owned and might include: smartphone, tablet, notebook/laptop or other technology that usually has the capability of utilising the school's wireless network. The device then has access to the wider internet which may include the school's learning platform and other cloud based services such as email and data storage.

All users should understand that the primary purpose of the use mobile/personal devices in a school context is educational. The mobile technologies policy should be consistent with and inter-related to other relevant school polices including but not limited to the safeguarding policy, behaviour policy, bullying policy, acceptable use policy, and policies around theft or malicious damage. Teaching about the safe and appropriate use of mobile technologies should be an integral part of the school's online safety education programme.

The school acceptable use agreements for staff, pupils and parents/carers will give consideration to the use of mobile technologies.

This school allows:

	School Devices			Personal Devices		
	School owned for single user	**School owned for multiple users**	**Authorised device[1]**	**Student owned**	**Staff owned**	**Visitor owned**
Allowed in school	*Yes*	*Yes*	*Yes*	*No*	*Yes*	*Yes*
Full network access	*Yes*	*Yes*	*Yes*	*No*	*No*	*No*
Internet only				*No*	*Yes - advise HEAD/ TIM*	*Yes – advise HEAD/TIM*
Network access				*No*	*No*	*No*

School owned/provided devices: *Who they will be allocated to?*

- *Year groups and classes share devices*

Where, when and how their use is allowed – times/places/in school/out of school

- *In classes under direction of professional teaching staff and support staff. If self-isolation/sickness due to COVID19 via Google Classroom lead by member of the teaching staff. Parents and carers are advised they are to be in the room when online teaching is taking place. Access using their own device at home via secured password to Google Classroom.*

If personal use is allowed

- *School provided device only school activities are to be completed and not used for personal use outside or inside the school by Teaching staff or pupils.* ***Examples such as*** **using a device to search for football results (unless part of a planned lesson), car tax (unless insuring School minibus by designated staff), employment (unless designated staff dealing with employment issues) Shopping (unless designated staff dealing with specific school request) entertainment and concerts (unless planning and booking school trips). Parents or carers are not to use school loaned pupils devices at home for their own purposes.**

Levels of access to networks/internet (as above)

- *Teaching staff and pupils have their own individual passwords to access learning materials inside and outside school. Networks are filtered and monitored. Levels of access are granted dependant on the user Teacher/Support staff/ Pupil/Guest user*

Personal devices:
Which users are allowed to use personal mobile devices in school (staff/pupils/visitors)?

- No one can use their personal device in school without the consent of the Executive Headteacher, Heads, each Executive Headteacher, Head will be aware of any teaching staff/users/using their personal devices for school use and

why. They should have this list and regularly review this and what information is being stored. **Personal devices should not be connected to the school Wi-Fi system unless express permission has been sought from the Head and they are aware of the reasoning. Should this occur, Head should have a list of these device and review it regularly and the information accessed and stored.**

- The HVT Staff Code of Conduct Policy specifies restrictions on where, when and how they may be used in school. The policy identifies designated areas such as the staff room.
- No pupils' mobile phones, smart watches are to be used in the school building. If older KS2 children have a mobile phone/smart device/watch this must be switched off and checked into either the school office or a securely locked location on arrival at the school site. Collection at the end of the school day and when clear of the school building the device can be switched on.

- All staff who bring a personal mobile phone into school are expected to keep these within a locked cupboard within the classroom, and in line with the school's online safety policy, only use these in designated areas within school and only in the absence of pupils e.g. – the school staff room or a school office. Mobile phones are prohibited from use in the classroom. Personal mobile phones are prohibited in being connected to the school's wifi unless explicit permission has been granted from the school's EHT/HT.
- All staff who choose to wear a smart watch are expected to use this in line with the school's online safety policy, only use these in designated areas within school and only in the absence of pupils. Smart watches are prohibited from use in the classroom. (e.g. you cannot answer a call on your smart watch or text message, the same as you would not be able to if you were using a mobile phone).
- All staff who use a school mobile device, including using it to take images, must ensure they
- use this in line with the school's online safety policy. "
- Pupil mobile devices/smart watches are kept in a secure locked location or in the school office.
- **No pupil mobile devices to be connected to the schools Wi-Fi system without express permission from the Head. Should this occur, Head should have a list of these device and review it regularly.**

Levels of access to networks/internet (as above)

- Teaching staff and pupils have their own individual passwords to access learning materials inside and outside school. Networks are filtered and monitored. Levels of access are granted dependant on the user Teacher/Support staff/ Pupil/Guest user/Supply Staff (dedicated Supply Staff logs on with access to a separate Teams area. This Teams area should not have personal data or names of staff or children and is purely for teaching and learning planning and resources. Long term supply staff have different arrangements and have Teaching Assistant level access.

Network/broadband capacity

- *This is monitored by the network providers (RM) and regularly reviewed*
- If a Head has deemed it necessary for staff to connect to the network, our network providers (RM) will offer technical support to ensure they can connect safely from inside and outside school to continue teaching. • Filtering of the internet connection to these devices

Data Protection

- School have the right to take, examine and search users devices in the case of misuse (England only) – N.B. this must also be included in the Behaviour Policy.

Taking/storage/use of images

- In consultation with the Executive Headteacher, Head all school staff, trainee teachers, pupils and volunteers are allowed to take digital/video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment; the personal equipment of staff should not be used for such purposes.

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents/carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for online-bullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website/social media/local press
- In accordance with guidance from the Information Commissioner's Office, parents/carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published/made publicly available on social networking sites, nor should parents/carers comment on any activities involving other pupils in the digital/video images.
- Once consent has been given staff and volunteers are allowed to take digital/video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment; the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital/video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission
- Once consent has been given photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Student's/Pupil's work can only be published with the permission of the student/pupil and parents or carers.

Data Protection

The Trust manages Data Protection in line with legislation and its Data Protection Policy

Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the school currently considers the benefit of using these technologies for education outweighs their risks/disadvantages:

Communication Technologies	Staff & other adults				Pupils				
	Not allowed	Allowed	Allowed at certain times and in designated areas	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times For educational purposes	Allowed with staff Permission and stored at the start of the day	
Mobile phones may be brought to the school			√					√	
Use of mobile phones in lessons	√				√				
Use of mobile phones/watches in social time			√		√				
Taking photos on mobile phones/cameras				√	√				
Use of other mobile devices e.g. tablets, gaming devices				√	√				
Use of personal email addresses in school, or on school network	√				√				
Use of school email for personal emails	√				√				
Use of messaging apps			√		√				
Use of social media			√		√				
Use of blogs				√			√		

When using communication technologies, the school considers the following as good practice:

- The official school email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored. *Staff and pupils should therefore use only the school email service to communicate with others when in school, or on school systems (e.g. by remote access).*
- Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Any digital communication between staff and pupils or parents/carers (email, social media, chat, blogs, VLE etc) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or social media must not be used for these communications.
- Whole class/group email addresses may be used at KS1, while pupils at KS2 and above will be provided with individual school email addresses for educational use.
- Pupils should be taught about online safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

Social Media - Protecting Professional Identity

All schools, academies, MATs and local authorities have a duty of care to provide a safe learning environment for pupils and staff. Schools, MATs and local authorities could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, engage in online bullying, discriminate on the grounds of sex, race or disability or who defame a third party may render the school or local authority/MAT liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

The Trust provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school through:

- Ensuring that personal information is not published
- Training is provided including: 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 or Trust
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information

When official school social media accounts are established there should be:

- A process for approval by senior leaders
- Clear processes for the administration and monitoring of these accounts – involving at least two members of staff – one of these can be the TIM
  A school based code of behaviour for users of the accounts, including:
- Systems for reporting and dealing with abuse and misuse
- Understanding of how incidents may be dealt with under school disciplinary procedures

Personal Use:

- Personal communications are those made via a personal social media accounts. In all cases, where a personal account is used which associates itself with the school or impacts on the school, it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy
- Personal communications which do not refer to or impact upon the school are outside the scope of this policy
- Where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken
- The school permits reasonable and appropriate access to private social media sites
- KCSIE Online Checks when working at the Trust schools - Online searches are carried out on all shortlisted candidates for positions at Hales Valley Trust. The searches are carried out to identify any incidents or issues that have happened, and are publicly available online, which Hales Valley Trust might want to explore with the candidate at interview.

Monitoring of Public Social Media:

- As part of active social media engagement, it is considered good practice to pro-actively monitor the Internet for public postings about the school
- The school should effectively respond to social media comments made by others according to a defined policy or process

The school's use of social media for professional purposes will be checked regularly by the TIM and Online Safety Group to ensure compliance with the school policies. The TIM should be clear who is updating social media accounts so they can communicate with the correct person following a monitoring procedure.

Generative Artificial Intelligence (AI)

- The school will take steps to prepare pupils for changing and emerging technologies, e.g. generative AI and how to use them safely and appropriately with consideration given to pupils' age.
- The school will ensure its IT system includes appropriate filtering and monitoring systems to limit pupil's ability to access or create harmful or inappropriate content through generative AI.
- The school will ensure that pupils are not accessing or creating harmful or inappropriate content, including through generative AI.
- The school will take steps to ensure that personal and sensitive data is not entered into generative AI tools and that it is not identifiable.
- The school will make use of any guidance and support that enables it to have a safe, secure and reliable foundation in place before using more powerful technology such as generative AI.
- AI DPIA (Data Protection Impact Assessment) and AI noted on Privacy Policies.
- AI CSA images are illegal to possess, produce and view in the UK, the same as non-AI generated CSA images.

Dealing with unsuitable/inappropriate activities

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned from school and all other technical systems. Other activities e.g. cyber-bullying would be 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 Trust 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/or outside the school when using school equipment or systems. The Trust policy restricts usage as follows:

User Actions		Acceptable	Acceptable at certain times – Trusted staff for education purposes	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 N.B. Schools/academies should refer to guidance about dealing with self-generated images/sexting – UKSIC Responding to and managing sexting incidents and UKCIS – Sexting in schools and colleges					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 discrimination				X	
	Threatening behaviour, including promotion of physical violence or mental harm				X	X
	Promotion of extremism or terrorism				X	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	
Activities that might be classed as cyber-crime under the Computer Misuse Act: • Gaining unauthorised access to school networks, data and files, through the use of computers/devices • Creating or propagating computer viruses or other harmful files • Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords) • Disable/Impair/Disrupt network functionality through the use of computers/devices • Using penetration testing equipment (without relevant permission) N.B. Schools will need to decide whether these should be dealt with internally or by the police. Serious or repeat offences should be reported to the police. Under the Cyber-Prevent agenda the National Crime Agency has a remit to prevent young people						X

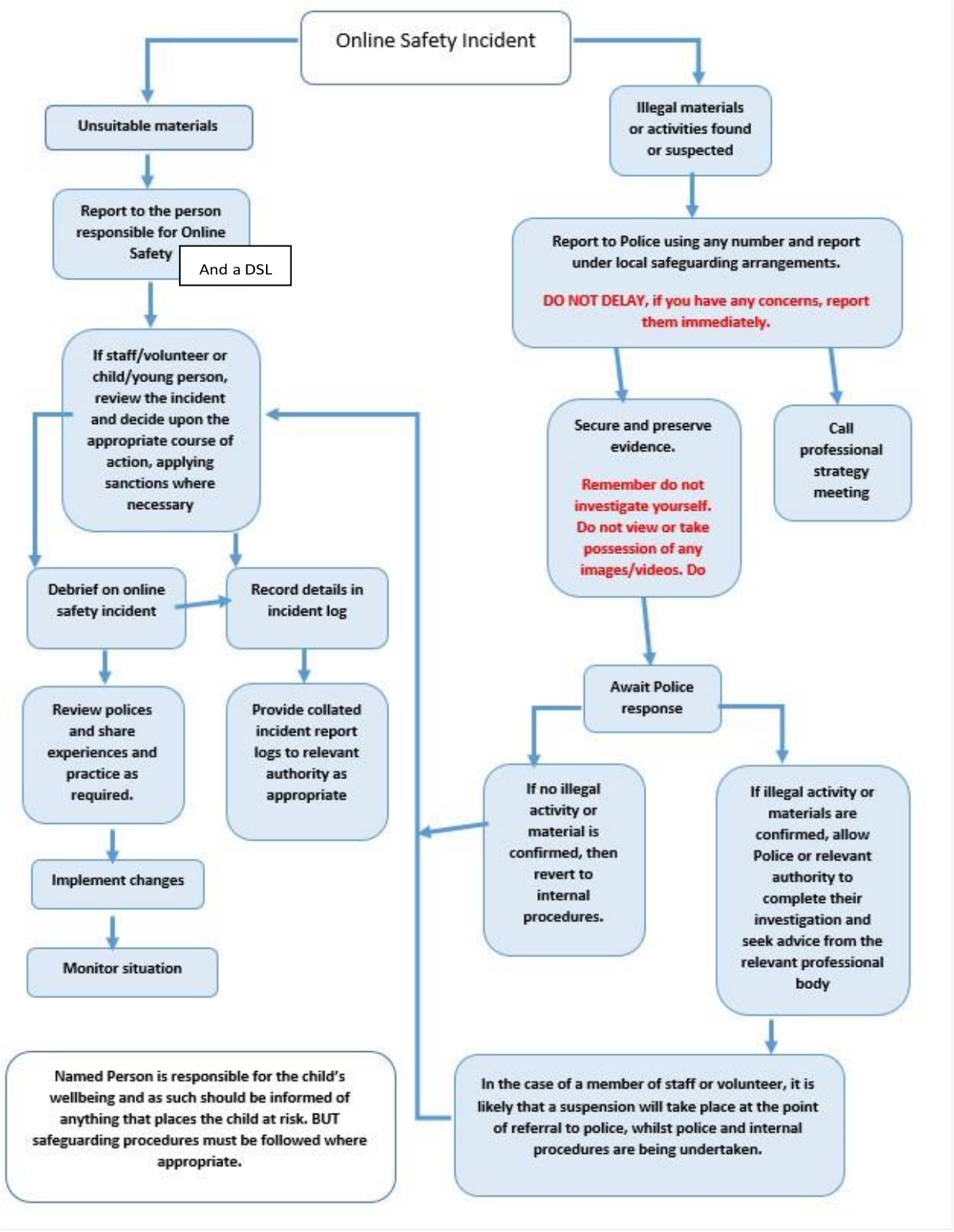
becoming involved in cyber-crime and harness their activity in positive ways – further information click here					
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school				X	
Revealing or publicising confidential or proprietary information (e.g. financial/personal information, databases, computer/network access codes and passwords)				X	
Unfair usage (downloading/uploading large files that hinders others in their use of the internet)				X	
Using school systems to run a private business				X	
Infringing copyright				X	
On-line gaming (educational)		X			
On-line gaming (non-educational)				X	
On-line gambling				X	
On-line shopping/commerce i.e school food shopping (BASC)		X			
File sharing – i.e. Via one drive/TEAMS for educational use		X			
Use of social media – i.e. for updating twitter, facebook, PTFA platforms		X			
Use of messaging apps – i.e.Parentmail for messaging whole cohorts		X			
Use of video broadcasting e.g. Youtube – i.e. trained staff may wish to resource for teaching purposes or with permissions share a video created within school		X			

Responding to incidents of misuse

This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities (see "User Actions" above).

Illegal Incidents

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right hand side of the Flowchart (below and appendix) for responding to online safety incidents and report immediately to the police.



Other Incidents

It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow school policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

In the event of suspicion, all steps in this procedure should be followed:

- Have more than one senior member of staff involved in this process including a DSL. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.

- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does, then appropriate action will be required and could include the following:
    - Internal response or discipline procedures ○ Involvement by Local Authority Group or national/local organisation (as relevant).
    - Police involvement and/or action
    - If content being reviewed includes images of child abuse, then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:
    - incidents of 'grooming' behaviour ○ the sending of obscene materials to a child
        - adult material which potentially breaches the Obscene Publications Act
        - criminally racist material ○ promotion of terrorism or extremism
    - offences under the Computer Misuse Act (see User Actions chart above) ○ other criminal conduct, activity or materials
- Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation. It is important that all of the above steps are taken as they will provide an evidence trail for the school and possibly the police and demonstrate that visits to these sites were carried out for safeguarding purposes. The completed form should be retained by the group for evidence and reference purposes.

School actions & sanctions

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour/disciplinary procedures.

	Actions/Sanctions								
Pupils Incidents	Refer to class teacher/tutor	Refer to Head of Department/Year/other	Refer to Executive Headteacher, Head	Refer to Police	Refer to technical support staff for action re filtering/security etc.	Inform parents/carers	Removal of network/internet access rights	Warning	Further sanction e.g. detention/exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable/inappropriate activities).		X	X	X	X	X	X	X	X

Unauthorised use of non-educational sites during lessons	X	X	X		X	X	X	X	X
Unauthorised/inappropriate use of mobile phone/digital camera/other mobile device	X	X	X		X	X		X	X
Unauthorised/inappropriate use of social media/ messaging apps/personal email	X	X	X		X	X		X	X
Unauthorised downloading or uploading of files	X	X	X		X	X	X	X	
Allowing others to access school network by sharing username and passwords	X	X	X		X	X	X	X	
Attempting to access or accessing the school network, using another pupil's account	X	X	X		X	X	X	X	X
Attempting to access or accessing the school network, using the account of a member of staff	X	X	X		X	X	X	X	X
Corrupting or destroying the data of other users	X	X	X		X	X	X	X	X
Sending an email, text or message that is regarded as offensive, harassment or of a bullying or racist nature	X	X	X		X	X	X	X	X
Continued infringements of the above, following previous warnings or sanctions	X	X	X		X	X	X	X	X
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	X	X	X		X	X	X	X	X
Using proxy sites or other means to subvert the school's filtering system	X	X	X		X	X	X	X	X
Accidentally accessing offensive or pornographic material and failing to report the incident	X	X	X		X	X		X	
Deliberately accessing or trying to access offensive or pornographic material	X	X	X	X	X	X	X	X	X
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act	X	X	X		X	X	X	X	X

Staff Incidents

Where a staff member misuses the Trust's IT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the Trust Disciplinary Policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.
The Trust will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

Example list of misusing the Trust IT system:

Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable/inappropriate activities).

Inappropriate personal use of the internet/social media/personal email
Unauthorised downloading or uploading of files
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account
Careless use of personal data e.g. holding or transferring data in an insecure manner
Deliberate actions to breach data protection or network security rules
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature
Using personal email/social networking/instant messaging/text messaging to carrying out digital communications with pupils
Actions which could compromise the staff member's professional standing
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school
Using proxy sites or other means to subvert the school's filtering system
Accidentally accessing offensive or pornographic material and failing to report the incident
Deliberately accessing or trying to access offensive or pornographic material
Breaching copyright or licensing regulations
Continued infringements of the above, following previous warnings or sanctions

Appendices

Current HVT primary acceptable use template

For Primary Pupils

The school has installed computers and provided Internet access to help our learning. I understand that the school may check my computer files and may monitor any Internet sites I visit.

These rules will keep everyone safe and help us to be fair to others. It is important that you read this policy carefully. If there is anything that you do not understand, please ask.

I agree that:

I will not share any of my passwords with anyone or use another person's password. If I find out someone else's password, I will tell that person and a member of the school staff, so they can change it.

I will use a password which contains some small and some big (capital) letters plus a number or a symbol *e.g. Skool5 or com**2er* and change it on a regular basis.

I will use the technology at school for learning. I will use the equipment properly and not interfere, change or delete someone else's work.

If I use a flash drive or other storage device, I will follow school guidelines on their use.

I will only e-mail people I know, or my teacher has approved.

If I attach a file to an email, it will not include any inappropriate materials (something I would not want my teacher to see or read) or anything that threatens the integrity of the school ICT system.

I will be respectful in how I talk to and work with others online and never write or participate in online bullying. If anyone sends me a message I do not like or feel uncomfortable about I will show it to my teacher or parent.

I will report any unpleasant material or messages sent to me. I understand my report would be confidential and would help protect other pupils and myself.

I will not download any programmes or games on to the school computers, netbooks or laptops unless I have permission to do so.

I will always check with a responsible adult before I share or publish images of myself, my friends or other people onto the internet.

I will not make audio or video recordings of another pupil or teacher without their permission.

When using sites on the internet, I will not give my name, home address, telephone/mobile number, pretend to be someone else or arrange to meet someone I do not know, unless my parent, carer or teacher has given permission.

I will always follow the 'terms and conditions' when using a website. The content on the web is someone's property and I will ask my teacher to help me get permission if I want to use information, pictures, video, music or sound files.

I will think carefully about what I read on the Internet, question if it is from a reliable source and use the information to help me answer any questions (I should not copy and paste the information and say it's my own work).

If I want to connect my own device to the school network, I will check with my teacher to see if it is possible.

If I use a school device at home I will follow the guidance as stated on the Pupil Loan Guardianship Form.

I am aware of the CEOP report button and know when to use it.

I know anything I do on the computer may be seen by someone else.

Signed:.....

PRINT NAME.....

Dated: .....

Alternative Template – for foundation/KS1

This is how we stay safe when we use computers:

- I will ask a teacher or suitable adult if I want to use the computers/tablets
- I will only use activities that a teacher or suitable adult has told or allowed me to use
- I will take care of computers/tablets and other equipment
- I will ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have done something wrong
- I will tell a teacher or suitable adult if I see something that upsets me on the screen
- I know that if I break the rules I might not be allowed to use a computer/tablet

Signed (child): ----------

Signed (parent): _____

Pupil Acceptable Use Agreement – for KS2

School policy

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe access to these digital technologies.

This acceptable use agreement is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other digital technologies for educational, personal and recreational use.
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and will have good access to digital technologies to enhance their learning and will, in return, expect the pupils to agree to be responsible users.

Acceptable Use Agreement

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

For my own personal safety:

- I understand that the *school* will monitor my use of the systems, devices and digital communications.
- I will keep my username and password safe and secure – I will not share it, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will be aware of "stranger danger", when I am communicating on-line.
- I will not disclose or share personal information about myself or others when on-line (this could include names, addresses, email addresses, telephone numbers, age, gender, educational details, financial details etc.)
- If I am asked to meet people in person (off-line) that I have communicated with on line, I will always tell a trusted adult immediately.
- 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 can report this to my parent or carer or any trusted adult in school.

I understand that everyone has equal rights to use technology as a resource and:

- I understand that the school systems and devices are primarily intended for educational use and that I will not use them for personal or recreational use unless I have permission.
- I will not try (unless I have permission) 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 systems or devices for on-line gaming, on-line gambling, internet shopping, file sharing, or video broadcasting (e.g. YouTube), unless I have permission of a member of staff to do so.

I will act as I expect others to act toward me:

- 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 own personal devices (mobile phones/USB devices etc (not recommended) in school if I have permission. I understand that, if I do use my own devices in the school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment.

- I will switch off my mobile device when entering the school premises and only switch my personal device back on when I leave the school premises.
- I understand the risks and will not upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I 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 hyperlinks in emails or any attachments to emails, unless I know and trust the person/organisation who sent the email, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will not install or attempt to install or store programmes of any type on any school device, nor will I try to alter computer settings.
- I will not use social media sites 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 and where they involve my membership of the school community (examples would be online-bullying, use of images or personal information).
- I understand that if I fail to comply with this acceptable use agreement, I may be subject to a sanction within school. This could include loss of access to the school network/internet, detentions, suspensions, contact with parents and in the event of illegal activities involvement of the police.)

Please complete the sections on the next page to show that you have read, understood and agree to the rules included in the acceptable use agreement. If you do not sign and return this agreement, access will not be granted to school systems and devices.

Student/Pupil Acceptable Use Agreement Form

This form relates to the *student/pupil* acceptable use agreement; to which it is attached.

Please complete the sections below to show that you have read, understood and agree to the rules included in the acceptable use agreement. If you do not sign and return this agreement, access will not be granted to school systems.

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

- I use the school systems and devices (both in and out of school)
- I use my own devices in the school (when allowed)
- I use my own equipment out of the 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, Google classroom, website etc.

Name of Pupil: ----------

Group/Class: ----------

Signed: ----------

Date: ----------

Parent/Carer Countersignature (optional) _____

HVT Parent/Carer Acceptable Use Agreement

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies provide powerful tools, which open up new opportunities for everyone. They can stimulate discussion,

promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

This acceptable use agreement is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that parents and carers are aware of the importance of online safety and are involved in the education and guidance of young people with regard to their on-line behaviour.

The school will try to ensure that pupils will have good access to digital technologies to enhance their learning and will, in return, expect the pupils to agree to be responsible users. A copy of the pupil acceptable use agreement is attached to this permission form, so that parents/carers will be aware of the school expectations of the young people in their care.

Parents are requested to sign the permission form below to show their support of the school in this important aspect of the school's work.

Permission Form

Parent/Carers Name: ----------

Pupil Name: ----------

As the parent/carer of the above pupils, I give permission for my child to have access to the internet and to ICT systems at school.

Either: (KS2 and above)

I know that my child has signed an acceptable use agreement and has received, or will receive, online safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.

Or: (KS1)

I understand that the school has discussed the acceptable use agreement with my child and that they have received, or will receive, online safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.

I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.

I understand that my child's activity on the systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the acceptable use agreement.

I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's online safety.

As the school is collecting personal data by issuing this form, it should inform parents/carers as to:

This form (electronic or printed)
Who will have access to this form.
Where this form will be stored.
How long this form will be stored for.
How this form will be destroyed.

Signed: ----------

Date: _____

Use of Digital/Video Images

The use of digital/video images plays an important part in learning activities. Pupils and members of staff may use digital cameras to record evidence of activities in lessons and out of school. These images may then be used in presentations in subsequent lessons.

Where consent is provided images may also be used to celebrate success through their publication in newsletters, on the school website and occasionally in the public media. Where an image is publicly shared by any means, only your child's first name/initials will be used.

The school will comply with the Data Protection Act and request parent's/carers permission before taking images of members of the school. We will also ensure that when images are published that the young people cannot be identified by the use of their names.

In accordance with guidance from the Information Commissioner's Office, parents/carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published/made publicly available on social networking sites, nor should parents/carers comment on any activities involving other *pupils* in the digital/video images.

Parents/carers will be contacted on an annual basis to provide specific consent for the use of images.

As the school is collecting personal data by issuing this form, it should inform parents/carers as to:

This form (electronic or printed)	The images
Who will have access to this form.	Where the images may be published. Such as; Twitter, Facebook, the school website, local press, etc. (see relevant section of form below)
Where this form will be stored.	Who will have access to the images.
How long this form will be stored for.	Where the images will be stored.
How this form will be destroyed.	How long the images will be stored for.
	How the images will be destroyed.
	How a request for deletion of the images can be made.

Digital/Video Images Permission Form

Parent/Carers Name: Student/Pupil Name:

HVT Staff (and Volunteer) Acceptable Use Policy Agreement

Trust Policy

New technologies have become integral to the lives of children and young people in today's society, both within schools/academies and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe access to the internet and digital technologies at all times.

This acceptable use policy is intended to ensure:

- that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that staff are protected from potential risk in their use of technology in their everyday work.

The school will try to ensure that staff and volunteers will have good access to digital technology to enhance their work, to enhance learning opportunities for *pupils* learning and will, in return, expect staff and volunteers to agree to be responsible users.

Acceptable Use Policy Agreement

I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users. I recognise the value of the use of digital technology for enhancing learning and will ensure that pupils receive opportunities to gain from the use of digital technology. I will, where possible, educate the young people in my care in the safe use of digital technology and embed online safety in my work with young people.

For my professional and personal safety:

- I understand that the *school* will monitor my use of the school digital technology and communications systems.
- I understand that the rules set out in this agreement also apply to use of these technologies (e.g. laptops, email, Google Classroom etc.) out of school, and to the transfer of personal data (digital or paper based) out of school
- I understand that the school digital technology systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the Trust.
- School Staff - I will ensure if I have guardianship of a school owned device I will sign a Guardianship Agreement.
- School Staff - I will ensure if I have guardianship of school owned portable devices that I ensure I scan these in and out of the school premises via the InVentry signing in and out system. I will speak to the school Technician if I cannot locate my device on the system.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may find it.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.

I will be professional in my communications and actions when using *school* systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and/or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital/video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (e.g. on the school website/VLE) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only use social networking sites in school in accordance with the Trust's policies.

- I will only communicate with pupils and parents/carers using official school systems. Any such communication will be professional in tone and manner.
- I will not engage in any on-line activity that may compromise my professional responsibilities.

The Trust has the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- When I use my mobile 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 will also follow any additional rules set by the school about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- I will not use personal email addresses on the school ICT systems.
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will ensure that my data is regularly backed up, in accordance with relevant school policies.
- I will not upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, terrorist or extremist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not 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 not try (unless I have permission) 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 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, unless this is allowed in school policies.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the Trusts Information Security Policy Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based documents containing personal data must be held in lockable storage.
- I understand that Data Protection Policy requires that any staff or student/pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by trust policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the internet in my professional capacity or for school sanctioned personal use:

- I will 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 download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of the *school*:

- I understand that this acceptable use policy applies not only to my work and use of school digital technology equipment in school, but also applies to my use of school systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school.
- I understand that if I fail to comply with this acceptable use agreement, I could be subject to disciplinary action. This could include a warning, a suspension, and in the event of illegal activities the involvement of the police.

I have read and understand the above and agree to use the school digital technology systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Staff/Volunteer Name: ----------

Signed: ----------

Date:

HVT Acceptable Use Agreement for Community Users

This acceptable use agreement is intended to ensure:

- that community users of school digital technologies will be responsible users and stay safe while using these systems and devices
- that school systems, devices and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that users are protected from potential harm in their use of these systems and devices

Acceptable Use Agreement

I understand that I must use school systems and devices in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems, devices and other users. This agreement will also apply to any personal devices that I bring into the school:

- I understand that my use of school systems and devices will be monitored
- I will not use a personal device that I have brought into school for any activity that would be inappropriate in a school setting.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, terrorist and extremist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not 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 illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.
- I will not access, copy, remove or otherwise alter any other user's files, without permission.
- I will ensure that if I take and/or publish images of others I will only do so with their permission. I will not use my personal equipment to record these images, without permission. If images are published it will not be possible to identify by name, or other personal information, those who are featured.
- I will not publish or share any information I have obtained whilst in the school on any personal website, social networking site or through any other means, unless I have permission from the school.
- I will not, without permission, 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 install or attempt to install programmes of any type on a school device, nor will I try to alter computer settings, unless I have permission to do so.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I will 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 download or distribute copies (including music and videos).
- I understand that if I fail to comply with this acceptable use agreement, the school has the right to remove my access to school systems/devices

I have read and understand the above and agree to use the school digital technology systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

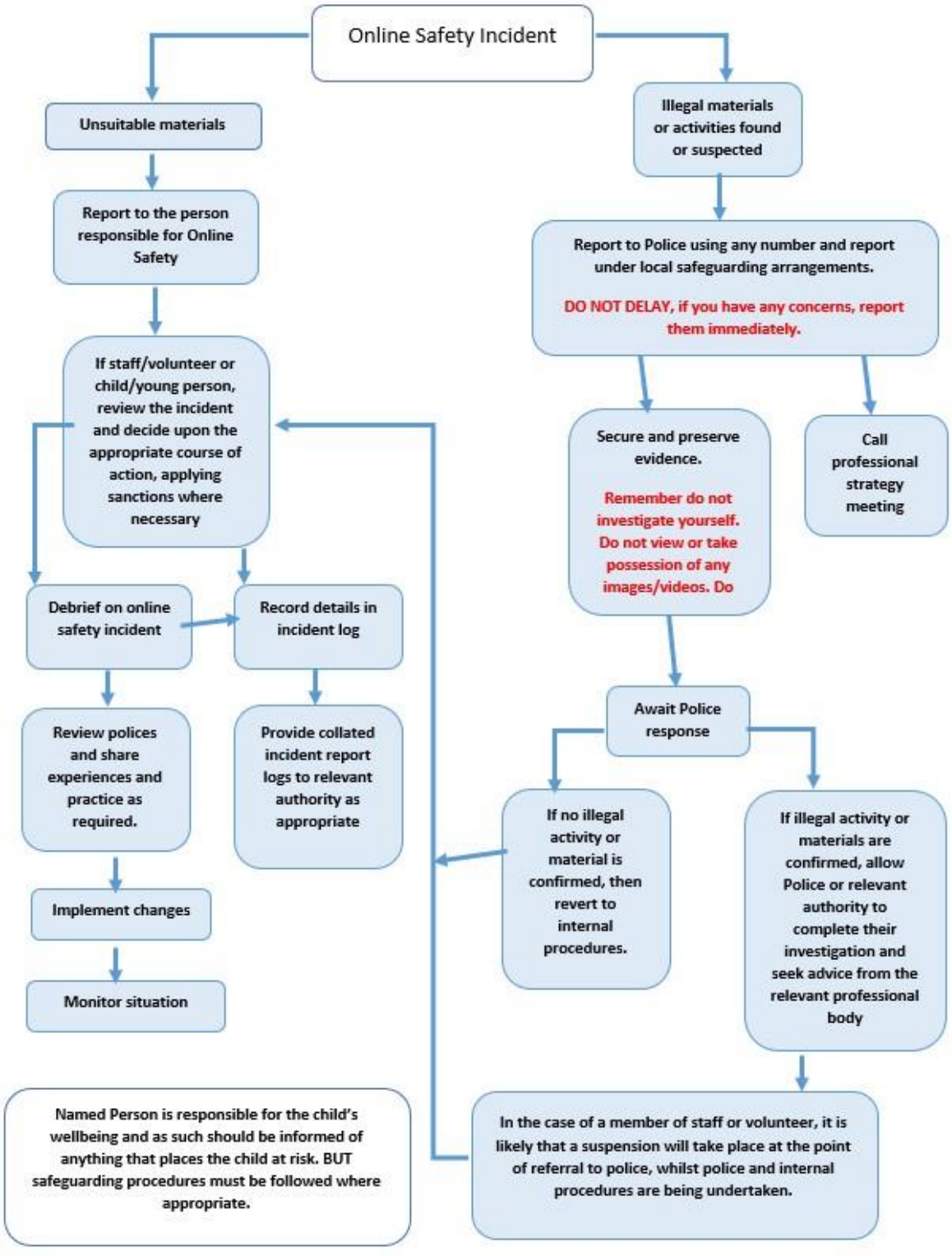
As the school is collecting personal data by issuing this form, it should inform community users about:

Who will have access to this form.	How this form will be destroyed.
Where this form will be stored.	How long this form will be stored for.

Name: ---------- Signed: _____

Date:……..

Responding to incidents of misuse – flow chart



NOTE:

The incident log at Hales Valley Trust is via CPOMS

Legislation

This policy is based on the Department for Education's (DfE) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- Relationships and sex education
- Searching, screening and confiscation

It also refers to the DfE's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

The policy also takes into account the National Curriculum computing programmes of study.

This policy complies with our funding agreement and articles of association.

Links to other organisations or documents

The following links may help those who are developing or reviewing a school online safety policy and creating their online safety provision:

UK Safer Internet Centre

Safer Internet Centre – https://www.saferinternet.org.uk/

South West Grid for Learning - https://swgfl.org.uk/products-services/online-safety/

Childnet – http://www.childnet-int.org/

Professionals Online Safety Helpline - http://www.saferinternet.org.uk/about/helpline

Revenge Porn Helpline - https://revengepornhelpline.org.uk/

Internet Watch Foundation - https://www.iwf.org.uk/

Report Harmful Content - https://reportharmfulcontent.com/

CEOP

CEOP - http://ceop.police.uk/

ThinkUKnow - https://www.thinkuknow.co.uk/

Others

LGfL – Online Safety Resources

Kent – Online Safety Resources page

INSAFE/Better Internet for Kids - https://www.betterinternetforkids.eu/

UK Council for Internet Safety (UKCIS) - https://www.gov.uk/government/organisations/uk-council-for-internet-safety

Netsmartz - http://www.netsmartz.org/

Tools for Schools

Online Safety BOOST – https://boost.swgfl.org.uk/

360 Degree Safe – Online Safety self-review tool – https://360safe.org.uk/

360Data – online data protection self-review tool: www.360data.org.uk

SWGfL Test filtering - http://testfiltering.com/

UKCIS Digital Resilience Framework - https://www.gov.uk/government/publications/digital-resilience-framework

Bullying/Online-bullying/Sexting/Sexual Harassment

Enable – European Anti Bullying programme and resources (UK coordination/participation through SWGfL & Diana Awards) - http://enable.eun.org/

SELMA – Hacking Hate - https://selma.swgfl.co.uk

Scottish Anti-Bullying Service, Respectme - http://www.respectme.org.uk/ Scottish Government - Better relationships, better learning, better behaviour - http://www.scotland.gov.uk/Publications/2013/03/7388 DfE - Cyberbullying guidance - https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/374850/Cyberbullying_Advice_for_Headteachers_and_School_Staff_121114.pdf

Childnet – Cyberbullying guidance and practical PSHE toolkit: http://www.childnet.com/our-projects/cyberbullying-guidance-and-practical-toolkit

Childnet – Project deSHAME – Online Sexual Harrassment

UKSIC – Sexting Resources

Anti-Bullying Network – http://www.antibullying.net/cyberbullying1.htm

Ditch the Label – Online Bullying Charity

Diana Award – Anti-Bullying Campaign

Social Networking

Digizen – Social Networking

UKSIC - Safety Features on Social Networks

Children's Commissioner, TES and Schillings – Young peoples' rights on social media

Curriculum

SWGfL Evolve - https://projectevolve.co.uk

UKCCIS – Education for a connected world framework

Teach Today – www.teachtoday.eu/ Insafe

- Education Resources

Data Protection

360data - free questionnaire and data protection self review tool

ICO Guides for Education (wide range of sector specific guides)

DfE advice on Cloud software services and the Data Protection Act

IRMS - Records Management Toolkit for Schools

NHS - Caldicott Principles (information that must be released)

ICO Guidance on taking photos in schools Dotkumo

- Best practice guide to using photos

Professional Standards/Staff Training

DfE – Keeping Children Safe in Education

DfE - Safer Working Practice for Adults who Work with Children and Young People

Childnet – School Pack for Online Safety Awareness

UK Safer Internet Centre Professionals Online Safety Helpline

Infrastructure/Technical Support

UKSIC – Appropriate Filtering and Monitoring

SWGfL Safety & Security Resources

Somerset - Questions for Technical Support

NCA – Guide to the Computer Misuse Act

NEN – Advice and Guidance Notes

Working with parents and carers

Online Safety BOOST Presentations - parent's presentation

Vodafone Digital Parents Magazine

Childnet Webpages for Parents & Carers

Get Safe Online - resources for parents

Teach Today - resources for parents workshops/education

Internet Matters

Prevent

Prevent Duty Guidance

Prevent for schools – teaching resources

NCA – Cyber Prevent Childnet
– Trust Me

Research

Ofcom –Media Literacy Research

Further links can be found at the end of the UKCIS Education for a Connected World Framework

Glossary of Terms

AUP/AUA	Acceptable Use Policy/Agreement – see templates earlier in this document
CEOP	Child Exploitation and Online Protection Centre (part of National Crime Agency, UK Police, dedicated to protecting children from sexual abuse, providers of the Think U Know programmes.
CPD	Continuous Professional Development
FOSI	Family Online Safety Institute
ICO	Information Commissioners Office
ICT	Information and Communications Technology
INSET	In Service Education and Training
IP address	The label that identifies each computer to other computers using the IP (internet protocol)
ISP	Internet Service Provider
ISPA	Internet Service Providers' Association
IWF	Internet Watch Foundation
LA	Local Authority
LAN	Local Area Network
MAT	Multi Academy Trust
MIS	Management Information System
NEN	National Education Network – works with the Regional Broadband Consortia (e.g. SWGfL) to provide the safe broadband provision to schools across Britain.
Ofcom	Office of Communications (Independent communications sector regulator)
SWGfL	South West Grid for Learning Trust – the Regional Broadband Consortium of SW Local Authorities – is the provider of broadband and other services for schools and other organisations in the SW
TUK	Think U Know – educational online safety programmes for schools, young people and parents.
UKSIC	UK Safer Internet Centre – EU funded centre. Main partners are SWGfL, Childnet and Internet Watch Foundation.
UKCIS	UK Council for Internet Safety
VLE	Virtual Learning Environment (a software system designed to support teaching and learning in an educational setting,
WAP	Wireless Application Protocol

A more comprehensive glossary can be found at the end of the UKCIS Education for a Connected World Framework