Online Safety Policy

Policy Tracker – Responsibility for monitoring this policy: Operations and IT (Reviewed annually – date of next review Autumn 27)			
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	September 2024
September 2025 Review	Sally Bloomer	Estates Manager and IT Lead	October 2025
September 2026 Review	Sally Bloomer/Senior Digital Leads	Estates Manager and IT Lead	

Contents

Contents	Page Number
1. Development/Monitoring/Review of this Policy	4
1.1 Schedule for Development/Monitoring/Review	4
2.Scope of the Policy	5
2.1 Links with Other Policies	5
3. Aims and Area of Online Safety Risk	5
3.1 The 4 Key Categories of Risk	5
3.2 Online Risks Associated with Serious Violence	6
3.3 Harmful Online Communities	6
3.4 Cyber Choices	6
3.5 Extra-Familial Harm	6
3.6 AI Risk Assessment and Approval	6
4. Roles and Responsibilities	7
4.1 Board of Directors	7
4.2 Executive Headteacher, Headteacher and Senior Leaders	7
4.3 Senior Digital Lead and/or Online Safety Lead	7
4.4 Trust IT Lead and Senior Technician	8
4.5 Teaching and Support Staff	8
4.6 Designated Safeguarding Leads/Online Safety Lead	8
4.7 Trust Online Safety Group	8
4.8 Pupils	9
4.9 Parents/Carers	9
4.10 Community Users	9
4.11 Human Oversight and Professional Judgment	9
5. Educating Pupils about Online Safety	10
6. Educating Parents/Carers about Online Safety	11
7. Use of Digital and Video Images	11
8. Cyberbullying	12
9. Examining Electronic Devices	12
10. Artificial Intelligence (AI), Generative AI and Online Safety	13
10.1 AI Safeguarding Risks	12
10.2 AI Incident Reporting	14
11. Child-on-Child Sexual Abuse and Harassment	14
12. Grooming and Exploitation	15
13. Child Sexual Exploitation (CSE) and Child Criminal Exploitation (CCE)	15
14. Radicalisation	15
15. Mental Health	15
16. Online Hoaxes and Harmful Online Challenges	15
17. Acceptable Use of the Internet in School	16
17.1 Pupils Using Mobile Devices in School	16
17.2 Staff Using Mobile Devices in School	16
17.3 How the School Will Respond to Issues of Misuse	17
18. Education and Training – Staff/Trustees/Volunteers	17
19. Technical – Infrastructure/Equipment, Filtering and Monitoring, Security	17
20. Data Protection	18

Appendices	
Appendix 1: Mobile Technologies (Including BYOD/BYOT)	19
Appendix 2: Communication	20
Appendix 3: Social Media – Protecting Professional Identity	21
Appendix 4: Managing Unsuitable/Inappropriate Activities	22
Appendix 5: Responding to Incidents of Misuse	24
Appendix 6: Pupil Acceptable Use Agreement	28
Appendix 7: HVT Parent/Carer Acceptable Use Agreement	30
Appendix 8: HVT Staff (and Volunteer) Acceptable Use Policy Agreement	32
Appendix 9: HVT Acceptable Use Agreement for Community Users	35
Appendix 10: Links to Other Organisations or Documents	36

1. Development/Monitoring/Review of this Policy

This online safety policy has been reviewed by the Estates manager and IT Lead and in consultation with the following:

- Executive Headteachers, Headteachers and senior leaders
- 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.

1.1 Schedule for Development/Monitoring/Review

This online safety policy was approved by the Curriculum and Standards Committee on:	
The implementation of this online safety policy will be monitored by the:	*Governors, DOE, 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 also be reviewed following any significant changes to statutory guidance, including Keeping Children Safe in Education, DfE Artificial Intelligence Guidance, UK Safer Internet Centre Guidance, Filtering and Monitoring Standards, cyber security standards or emerging AI-related safeguarding risks. The next anticipated review date will be: **September 27**	*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 non-compliant 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/carers
    - staff

2. 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 Act 1996 and the Education and Inspections Act 2006 empowers Headteachers 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 Education Act 2011, 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:

- Keeping Children Safe in Education, and its advice for schools on:
- Teaching online safety in schoolshttps://www.gov.uk/government/publications/preventing-and-tackling-bullying
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- Relationships and sex education (SRE) and Health Education – up to August 2026
- Searching, screening and confiscation
- Generative artificial intelligence (AI) in education - GOV.UK

It also refers to the DfE's guidance on protecting children from radicalisation.
It reflects existing legislation, including the Equality Act 2010.
The policy also considers the National Curriculum computing programmes of study and complies with our funding agreement and articles of association.

2.1 Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure
- ICT and internet acceptable use policy

3. Aims and Areas of Online Safety Risk

Our Trust aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Identify and support groups of pupils that are potentially at greater risk of harm online than others
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones')
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

3.1 The 4 Key Categories of Risk

Our approach to online safety is based on addressing the following categories of risk:

1. **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, misinformation, disinformation including AI-generated misinformation, deepfake images, deepfake video, AI-generated voice cloning, AI-generated nude and semi-nude images, manipulated content, synthetic media, conspiracy theories, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism
2. **Contact** – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit the user for sexual, criminal, financial or other purposes
3. **Conduct** – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and
4. **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scams

Children with particular skills and interest in computing and technology may inadvertently or deliberately stray into cyber-dependent 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.

3.2 Online Risks Associated with Serious Violence

The Trust recognises that online activity can contribute to or facilitate serious violence and other safeguarding concerns. Children may be exposed to harmful content that promotes violence, weapons, criminal activity, gang affiliation or extremist ideologies, or people may use online platforms to make threats, intimidate others or organise harmful behaviour. Online interactions may also be linked to child criminal exploitation, county lines activity and peer-on-peer abuse. Staff should remain alert to indicators that a child may be at risk of involvement in serious violence, whether as a victim or perpetrator, and should report any concerns promptly to the Designated Safeguarding Lead. Where appropriate, concerns will be assessed alongside other safeguarding information and managed in accordance with the Trust's Child Protection and Safeguarding Policy, with referrals made to external agencies where necessary.

3.3 Harmful Online Communities

The Trust recognises that children may be exposed to harmful online communities or networks that encourage abuse, exploitation, discrimination, misogyny, self-harm, suicide, eating disorders, criminal behaviour, extremism or other harmful activities. These communities may exist across social media platforms, gaming environments, messaging services and other online spaces and may normalise harmful behaviour or encourage children to engage in activities that place them or others at risk. Staff should remain vigilant to indicators that a child may be engaging with harmful online communities and respond in accordance with the Trust's safeguarding procedures, seeking support from the Designated Safeguarding Lead where concerns arise.

3.4 Cyber Choices

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-children-safe/reporting-abuse/what-if-suspect-abuse/

3.5 Extra-familial Harm

The Trust recognises that safeguarding concerns can arise outside the family home and that children may experience harm in a range of community, peer and online settings. Extra-familial harm includes risks such as child criminal exploitation (CCE), child sexual exploitation (CSE), serious violence, county lines, harmful peer relationships, online grooming, radicalisation, and abuse occurring through social media, gaming platforms, messaging services or other online communities. Online activity may both facilitate and conceal these forms of harm. Staff should remain professionally curious, be alert to indicators that a child may be at risk both online and offline, and report concerns promptly to the Designated Safeguarding Lead. Where appropriate, safeguarding responses should take account of the wider contexts in which children live, learn and socialise, working in partnership with external agencies to reduce risk and promote children's safety and wellbeing.

3.6 AI Risk Assessment and Approval

Prior to implementation, all AI systems, platforms or services used by the Trust will undergo appropriate review and approval processes.

This will include consideration of:

- Safeguarding implications.
- Online safety risks.
- Cyber security risks.
- Data protection compliance.
- Privacy and information governance requirements.
- Age appropriateness.
- Filtering and monitoring requirements.
- The potential for misuse or harmful content generation.

Where appropriate, the Trust will complete a Data Protection Impact Assessment (DPIA) and maintain records within its AI Register.

No AI tool may be introduced for staff or pupil use unless appropriate safeguarding, cyber security and data protection assessments have been completed and approval has been granted through Trust procedures.

4. Roles and Responsibilities

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

4.1 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, we ensure our Trust has appropriate filtering and monitoring systems in place and regularly review their effectiveness. They 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. The Trustees consider the number of and age range of our 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 DFO 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 Anchor reports
- monitor of filtering/change control logs via the DFO report
- reporting to Curriculum and standards committee
- Check status of schools 360 Safe progress and awards.

4.3 Executive Headteacher, Heads and Senior Leaders

- The Executive Headteacher, Head Teacher or Head of School 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 Senior Digital leader and/or Online Safety lead in each school
- The Executive Headteacher, Head Teacher or Head of School 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, Head Teacher or Head of School and Senior Leaders are responsible for ensuring that the Senior Digital leader and/or 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, Head Teacher or Head of School 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 Senior Digital leader and/or Online Safety lead. The IT Leaders Online Safety Meetings are led by a Senior Digital Leader from one of the schools.
- 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).

4.3 Senior Digital Lead and/or Online Safety Lead (ideally should have DSL status)

- leads the Online Safety work in school
- maintains an overview of the Trust Digital Strategy to meet the DFE standards.
- 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 IT department
- 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 the Trust IT lead 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).

4.4 Trust IT lead and Senior Technician

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, Head Teacher or Head of School, 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).

4.5 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/ Head Teacher or Head of School /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

4.6 Designated Safeguarding Lead/Online Safety Lead

Designated Safeguarding Leads should be aware that online safety concerns may indicate wider safeguarding issues and should be managed in line with local safeguarding partnership arrangements and the Trust's Child Protection and Safeguarding Policy. Where concerns suggest that a child may require additional support or be at risk of significant harm, the Designated Safeguarding Lead will consider the appropriate course of action, including Family Help, referral to Children's Social Care, the Police or other relevant agencies, in accordance with local safeguarding thresholds and statutory guidance. 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).

They 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

4.7 Trust Online Safety Group

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 another 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 Head Teacher or Head of School of their school.
- Respond to common issues within their school.

4.8 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

4.9 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

4.10 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.)

4.11 Human Oversight and Professional Judgement

Artificial Intelligence may support decision-making and administrative processes but must never replace professional judgement. All staff remain responsible for:

- Verifying the accuracy of AI-generated information.
- Checking content for bias, inaccuracies, safeguarding concerns or misinformation.
- Applying professional judgement when using AI outputs.
- Ensuring safeguarding decisions are informed by appropriate human review.

No safeguarding, welfare, behaviour, attendance, SEND, disciplinary or educational decision affecting a child shall be made solely on the basis of an AI-generated recommendation. Human oversight will remain central to all decision-making processes.

5. Educating Pupils about Online Safety

Pupils will be taught about online safety as part of the curriculum.
At Hales Valley Trust we follow the National Curriculum computing programmes of study and the government's guidance on relationships education, relationships and sex education (RSE) and health education (for teaching until 31 August 2026).

All schools have to teach:

- Relationships education and health education in primary schools

In **Key Stage 1**, pupils will be taught to:

- Use technology safely and respectfully, keeping personal information private
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

Pupils in **Key Stage 2** will be taught to:

- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact
- Be discerning in evaluating digital content

By the **end of primary school**, pupils will know:

- That the internet can be a negative place where online abuse, trolling, bullying and harassment can take place, which can have a negative impact on mental health
- That people sometimes behave differently online, including by pretending to be someone they are not
- That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others, including when we are anonymous
- The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them
- How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met
- How information and data are shared and used online
- How to be a discerning consumer of information online including understanding that information, including that from search engines, is ranked, selected and targeted
- What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context)
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know
- The benefits of rationing time spent online, the risks of excessive time spent on electronic devices and the impact of positive and negative content online on their own and others' mental and physical wellbeing
- Why social media, computer games and online gaming have age restrictions and how to manage common difficulties encountered online
- How to consider the effect of their online actions on others and know how to recognise and display respectful behaviour online and the importance of keeping personal information private
- Where and how to report concerns and get support with issues online

The Trust is committed to fostering a culture in which all children feel safe, listened to and supported when raising concerns about their online experiences. Pupils will be encouraged to speak to a trusted adult if they encounter anything online that makes them feel unsafe, uncomfortable or worried, whether the concern relates to themselves or another child. Staff will ensure that all reports are taken seriously, responded to promptly and managed in accordance with the Trust's safeguarding procedures, recognising that children may not always feel ready or able to disclose concerns immediately.

The safe use of social media and the internet will also be covered in other subjects where relevant. The Trust will provide age-appropriate education to pupils regarding what artificial intelligence is the benefits and limitations of AI technologies, deepfakes and manipulated media, misinformation and disinformation, ethical use of AI, digital consent, respectful behaviour and reporting concerns relating to AI-generated content.

Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and pupils with SEND.

6. Educating Parents/Carers about Online Safety

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 schools in the Trust will raise parents/carers' awareness of internet safety in letters or other communications home, and in information via our websites. This policy will also be shared with parents/carers.

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

- Curriculum activities
- Letters, newsletters, website, Learning Platform support
- 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 , "Wake up Wednesday" posters.

The schools will let parents/carers know:

- What systems the school uses to filter and monitor online use
- What their children are being asked to do online, including the sites they will be asked to access and who from the school (if anyone) their child will be interacting with online

If parents/carers have any queries or concerns in relation to online safety, these can be raised with the class teachers, headteacher and/or the DSL.

Concerns or queries about this policy can be raised with any member of staff or the headteacher.

7. 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.

8. Cyberbullying

Cyberbullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of 1 person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.)
It 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. (See also the school's behaviour policy)
To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and encourage them to do so, including where they are a witness rather than the victim.
The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Class teachers will discuss cyber-bullying with their classes.
Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.
All staff receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training. The school also sends information/leaflets on cyber-bullying to parents/carers so they are aware of the signs, how to report it and how they can support children who may be affected.
In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.
The DSL will report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

9. Examining Electronic Devices

The headteacher, and any member of staff authorised to do so by the headteacher, can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

- Poses a risk to staff or pupils, and/or
- Is identified in the school rules as a banned item for which a search can be carried out, and/or
- Is evidence in relation to an offence

Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:

- Assess how urgent the search is, and consider the risk to other pupils and staff. If the search is not urgent, they will seek advice from the headteacher/DSL. They will explain to the pupil why they are being searched, and how the search will happen; and give them the opportunity to ask questions about it
- Seek the pupil's co-operation

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on an electronic device that they have confiscated where they believe there is a 'good reason' to do so.
When deciding whether there is a 'good reason' to examine data or files on an electronic device, the staff member should reasonably suspect that the device has, or could be used to:

- Cause harm, and/or
- Undermine the safe environment of the school or disrupt teaching, and/or
- Commit an offence

If inappropriate material is found on the device, it is up to the head teacher to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding whether there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to any person, and/or
- The pupil and/or the parent/carer refuses to delete the material themselves

If a staff member **suspects** a device **may** contain an indecent image of a child (also known as a nude or semi-nude image), they will:

- **Not** view the image
- Confiscate the device and report the incident to the DSL (or equivalent) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on screening, searching and confiscation and the UK Council for Internet Safety (UKCIS) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

Any searching of pupils will be carried out in line with:

- The DfE's latest guidance on searching, screening and confiscation
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- Our behaviour policy

10. Artificial Intelligence (AI), Generative AI and Online Safety

Artificial Intelligence (AI) technologies are becoming increasingly common within education and wider society. Hales Valley Trust recognises that AI can provide valuable opportunities to support teaching, learning, administration and accessibility. However, AI technologies also present emerging safeguarding, online safety, cyber security and data protection risks which require careful management. The Trust is committed to ensuring that all AI systems are used safely, ethically and lawfully.

Generative AI tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Gemini.

10.1 AI Safeguarding Risks

The Trust recognises that AI technologies can be misused to create, manipulate or distribute harmful content and may expose pupils and staff to new safeguarding risks.

These risks may include:

- Deepfake images, videos and audio recordings.
- AI-generated abuse and harassment.
- AI-assisted cyberbullying.
- AI-enabled grooming and exploitation.
- Impersonation using synthetic voice, image or video technology.
- AI-generated misinformation and disinformation.
- Synthetic imagery designed to manipulate or deceive.
- AI-generated nude or semi-nude images.
- Identity theft and fraud.
- Harmful content generated through AI chatbots or image generators.
- The creation, possession or sharing of illegal AI-generated child sexual abuse material.

The Trust will ensure that pupils are educated about these risks through its online safety, computing, RSHE and safeguarding curriculum and that staff remain vigilant to emerging forms of AI-enabled abuse. Any concerns relating to AI-generated content will be treated in the same way as other safeguarding concerns.

Hales Valley Trust recognises that AI has many uses to help pupils learn but may also have the potential to be used to bully others. For example, in the form of 'deep fakes', where AI is used to create images, audio or video hoaxes that look real. This includes deep fake pornography: pornographic content created using AI to include someone's likeness.

Hales Valley Trust will treat any use of AI to bully pupils very seriously, in line with our anti-bullying and behaviour policies.
Staff should be aware of the risks of using AI tools while they are still being developed and should carry out a risk assessment where new AI tools are being used by the Trust, and where existing AI tools are used in cases which may pose a risk to all individuals that may be affected by them, including, but not limited to, pupils and staff.

- 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.

10.2 AI Incident Reporting

The Trust recognises that incidents involving artificial intelligence may present a safeguarding risk to children and young people. All AI-related concerns shall therefore be treated as safeguarding concerns where they involve pupils, vulnerable adults, harassment or bullying, deepfakes or manipulated media, grooming or exploitation, nude or semi-nude imagery, abuse, intimidation or threats and unauthorised use of personal information.

Where an AI-related concern is identified:

1. The concern must be reported immediately to the Designated Safeguarding Lead (DSL) or Deputy DSL.
2. Appropriate evidence should be preserved where safe and lawful to do so.
3. The concern must be recorded on CPOMS.
4. The DSL will assess whether the matter requires referral to external agencies, including the Police, Local Authority, LADO, Children's Services or the UK Safer Internet Centre.
5. AI-related incidents will be reviewed termly by safeguarding leaders to identify trends, emerging risks and required actions.

The Trust will maintain records of significant AI-related safeguarding concerns and use these records to inform staff training, pupil education and future risk assessments.

11. 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 online behaviour of this kind, 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.

Staff 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 this policy and the behaviour policy.

Each 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 this policy, the behaviour policy and the Child Protection and Safeguarding Policy.

12. 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 safeguarding and 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.

13. 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.

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.

14. Radicalisation

Radicalisation is the process where an individual moves toward supporting or engaging with extremist or groups, often developing extreme views that are a form of harm This process involves a person adopting beliefs that reject fundamental societal values and can lead to violence or support for terrorism, aiming to destroy others' rights or overturn democratic systems. 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 child protection and safeguarding policy.

15. 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.

16. 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.

17. Acceptable Use of the Internet in School

All pupils, parents/carers, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendices 6 to 9). Visitors will be expected to read and agree to the school's terms on acceptable use, if relevant.
Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.
We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above and restrict access through filtering systems where appropriate.
More information is set out in the acceptable use agreements in appendices 6 to 9.

17.1 Pupil Using Mobile Devices in School

Only pupils in Year 6 who walk to and from school alone, may bring mobile devices into school. this will include smart watches. Mobile devices to monitor medical needs i.e. diabetes monitor will be handed to the staff member responsible the child's needs. These will all be handed into to class teachers at the beginning of the day and returned at the end of day. This will include smart watches. They will be stored securely in the office. Pupils are not permitted to use them during:

- Lessons
- Clubs before or after school, or any other activities organised by the school

Any use of mobile devices in school by pupils must be in line with the acceptable use agreement (see appendices 6).

Any breach of the acceptable use agreement by a pupil may trigger disciplinary action in line with the school behaviour policy, which may result in the confiscation of their device.

17.2 Staff Using Work Devices Outside School

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping the device password-protected – strong passwords can be made up of 3 random words, in combination with numbers and special characters if required, or generated by a password manager
- Ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device (Bit locker)
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends
- Installing anti-virus and anti-spyware software
- Keeping operating systems up to date by promptly installing the latest updates
- Staff members must not use the device in any way that would violate the school's terms of acceptable use, as set out in appendix 3.
- Work devices must be used solely for work activities.

17.3 How the School Will Respond to Issues of Misuse

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our policies on behaviour and ICT Internet acceptable use. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate. Please see Appendix 4 – 5

Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures and staff code of conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident. Please see Appendix 4 – 5

The school will consider whether incidents that involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

18. Education & Training – Staff/Trustees/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 – included annually in safeguarding training. An audit of the online safety training needs of all staff will be carried out regularly.
- All new staff should receive online safety training and NCSC cyber security training as part of their induction programme, i.e. online safety module from National college 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 meetings and training sessions.
- The Online Safety Lead (or other nominated person such as a DSL) will provide advice/guidance/training to individuals as required.
- The DSL [and deputy/deputies] will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.
- **Trustees** complete 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 another relevant organisation such as through Governor Hub
    - Participation in school training/information sessions for staff or parents
    - National Online Safety online training and NCSC cyber security training.

19. Technical – Infrastructure/Equipment, Filtering and Monitoring, Security

The Trust 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 RM our Managed Service provider

    - RM provides school-wide filtering and monitoring solutions using RM SafetyNet for web filtering and Smoothwall Monitor for on-device e-Safety monitoring and alerting. RM has installed Smoothwall Monitor on all RM managed devices which detects safeguarding concerns and alerts a school-nominated member of staff by email or telephone in the most serious cases. Smoothwall Monitor training is available to all schools.

    - 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 Lead and 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.

    - The Trust will ensure that filtering and monitoring systems continue to protect users from risks associated with AI technologies.
      Annual reviews of filtering and monitoring arrangements will specifically consider:
      AI-powered websites and applications, generative AI tools, deepfake and synthetic media risks, AI-generated harmful content, the potential for AI systems to circumvent existing safeguarding controls.

All AI technologies used within the Trust must operate within existing safeguarding and monitoring arrangements and must not weaken established protections

- 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 . 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.
- 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. 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, 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).
- Any security breach/ loss of device etc should be reported as soon as noted within 24 to 48 hours to Head of Operations (or Estates &IT Lead if out of office) who will provide advice on the breach and where necessary will advise the school to report to the Trusts named DPO (Your IG).
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, workstations, 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).
- 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.
- 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 data in a few hours.
- 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 school's systems. AUP must be signed by the guest user.
- We do not allow USB flash drives or portable hard drives in any of our schools. All staff must use one drive to store and transfer files when working on them remotely. **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).

20. Data Protection

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

Appendix 1: 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, anti-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 consider the use of mobile technologies.

This Trust 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*	*No*	*Yes, with permission*
Network access				*No*	*No*	*No*

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. **Personal devices should not be connected to the school Wi-Fi system.** 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.
- 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.

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 have a dedicated Supply Staff log on with limited access for short periods.

Appendix 2: 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	llowed for selected staff	Not allowed	Allowed	Allowed at certain times or 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 (info@ only) may be regarded as safe and secure and is monitored. Staff to check this email service but do not respond from their personal emails. Respond through info@ only. 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.

Appendix 3: 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. The Trust and schools within the Trust 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 account. 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.

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

Appendix 4: Managing 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					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) Under the Cyber-Prevent agenda the National Crime Agency has a remit to prevent young people becoming involved in cyber-crime and harness their activity in positive ways – further information click here						X

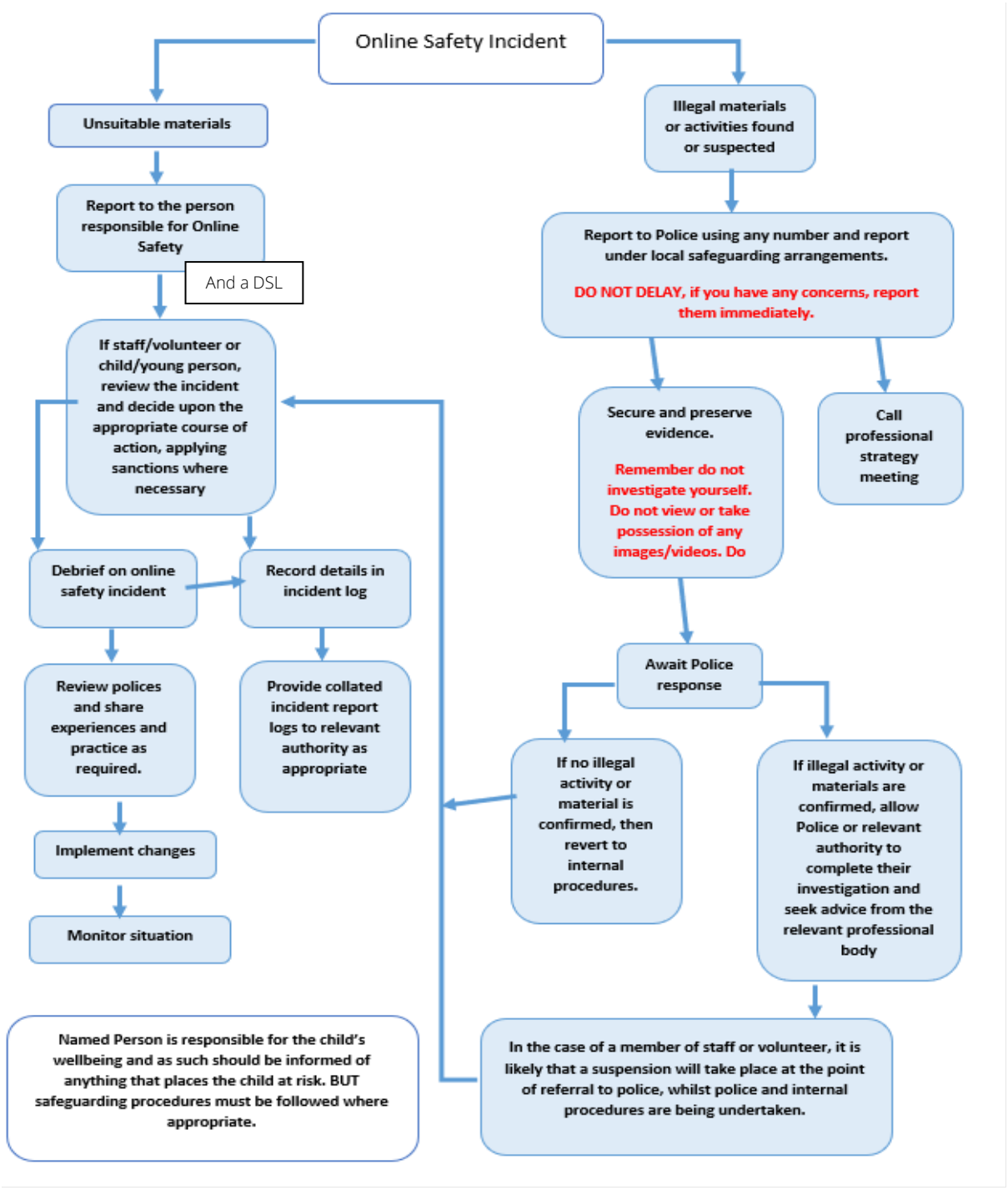
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school				X	
Revealing or publicising confidential or proprietary information (e.g. financial/personal information, databases, computer/network access codes and passwords)				X	
Unfair 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			

Appendix 5: 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 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/another 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

Appendix 6: Pupil Acceptable Use Agreement

School policy

Digital technologies have become integral to the lives of young people, both within schools and outside school. Young people should have an entitlement to safe access to these digital technologies.

This acceptable use agreement is intended to ensure:

- that pupils 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 intended for education and that I will not use them for personal use unless I have permission.
- I will not try 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, 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 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 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) 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
- I will not use any programmes or software that might allow me to bypass the filtering/security systems in place.
- 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, due to virus risk.

- 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 will follow the Online safety Policy and Behaviour policy if I am involved in incidents of inappropriate behaviour, that are covered in this agreement. This includes when I am out of school and where they involve my membership of the school community (for example: online-bullying, inappropriate use of images or personal information).
- I understand that if I do not follow this acceptable use agreement, I may be subject to a sanction within school, may involve parents support and other agencies. (See Behaviour policy and Online Safety policy)

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: ..... **Class:** ...

Signed: ..... **Date:** .....

Parent/Carer Countersignature (optional) .....

Appendix 7: 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)
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 parents communicate to school via school@lapal.dudley.sch.uk and responses will be received via this email address. Contacting staff via personal emails will not be responded to as school@lapal emails are monitored closely by senior and office staff.
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, the school will follow our retention policy and it will be stored in the main office for access by the Office manager and Senior staff.

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, the school will follow our retention policy and it will be stored in the main office until recorded on our Management Information System to record permissions - for access by the Office manager and Senior staff.

Parent/Carers name:…….Student/Pupil Name:…….

Signed ……..

Appendix 8: HVT Staff (and Volunteer) Acceptable Use Policy Agreement

This policy applies to all adult users of the school's systems. We trust you to use the ICT facilities sensibly, professionally, lawfully, consistent with your duties, with respect for your colleagues and I accordance with this policy.
It is important that you read this policy carefully. If there is anything that you do not understand, please discuss it with the Headteacher or your line manager. Once you have read and understood this policy thoroughly you should sign this document, retain a copy for your own records and return the original to the Office Manager.
Any inappropriate use of the school's internet and email systems whether under this policy or otherwise may lead to disciplinary action being taken against you under the appropriate disciplinary procedures which may include summary dismissal. Electronic information can be produced in court in the same way as oral or written statements.
Research Machines (RM) is contractually required to monitor the use of internet and email services it provides, in accordance with The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000. Traffic data and usage information may be recorded and may be used in disciplinary procedures if necessary. RM, Hales Valley Trust and the school reserve the right to disclose any information deemed necessary to satisfy any applicable law, regulation, legal process or governmental request. If there is any evidence that this particular policy is being abused by individuals, we reserve the right to withdraw from employees the facility to view, send and receive electronic communications or to access the internet.
All information relating to our pupils, parents and staff is personal. You must treat all school information with the utmost care whether held on paper or electronically. Official school systems must be used at all times.

Use of the Internet and Intranet

When entering an internet site, always read and comply with the terms and conditions governing its use. Be aware at all times that when visiting an internet site the unique address for the computer you are using (the IP address) can be logged by the site you visit, thus identifying your school. For your information, the following activities are criminal offences under the Computer Misuse Act 1990:

- Unauthorised access to computer material i.e. hacking
- Unauthorised modification of computer material; and
- Unauthorised access with intent to commit/facilitate the commission of further offences.

In line with this policy, the following statements apply:

- If you download any image, text or material check if it is copyright protected. If it is, then follow the school procedure for copyright material.
- Do not download any image, text or material which is inappropriate or likely to cause offence. If this happens accidentally report in to a senior member of staff.
- If you want to download any software, first seek permission from the Headteacher and/or RM. They should check that the source is safe and appropriately licensed.
- If you are involved in creating, amending or deleting web pages or content on the website, such actions should be consistent with your responsibilities and in the best interests of the school.

You should not:

- Introduce packet-sniffing software (i.e. software which is used to intercept data on a network) or password detecting software;
- Seek to gain access to restricted areas of the network;
- Knowingly seek to access data which you are not authorised to view;
- Carry out other hacking activities.

Electronic Mail

Care must be taken when using email as a means of communication as all expressions of fact, intention or opinion may implicate you and/or the school or Trust.
Internet and e-mail access is intended to be used for school business or professional development, any personal use is subject to the same terms and conditions and should be with the agreement of your head teacher. Your privacy and autonomy in your business communications will be respected. However, in certain circumstances it may be necessary to access and record your communications for the School's business purposes which include the following:

1. providing evidence of business transactions;
2. making sure the School's business procedures are adhered to;
3. training and monitoring standards of service;
4. preventing or detecting unauthorised use of the communications systems or criminal activities;
5. maintaining the effective operation of communication systems.

In line with this policy the following statements apply: -

- You should agree with recipients that the use of e-mail is an acceptable form of communication. If the material is confidential, privileged, or sensitive you should be aware that un-encrypted e-mail is not secure.
- Do not send sensitive personal data via email unless you are using a secure site or portal. It is good practice to indicate that the email is 'Confidential' in the subject line.
- Copies of emails with any attachments sent to or received from parents should be saved in a suitable secure directory.
- Do not impersonate any other person when using e-mail or amend any messages received.
- Sending defamatory, sexist or racist jokes or other unsuitable material via the internet or email system is grounds for an action for defamation, harassment or incitement to racial hatred in the same way as making such comments verbally or in writing.
- It is good practice to re-read e-mail before sending them as external e-mail cannot be retrieved once they have been sent.
- If the email is personal, it is good practice to use the word 'personal' in the subject header and the footer text should indicate if it is a personal email the school does not accept responsibility for any agreement the user may be entering into.
- Internet and e-mail access is intended to be used for school business or professional development, any personal use is subject to the same terms and conditions and should be with the agreement of your Headteacher.
- All aspects of communication are protected by intellectual property rights which might be infringed by copying. Downloading, copying, possessing and distributing material from the internet may be an infringement of copyright or other intellectual property rights.

Social Networking

The use of social networking sites for business and personal use is increasing. Access to social networking sites is blocked on the school systems, however a school can manage access by un-filtering specific sites, internet usage is still monitored.

School staff may need to request access to social networking sites for a number of reasons including:

- Advertising the school or managing an 'official' school presence,
- For monitoring and viewing activities on other sites
- For communication with specific groups of adult users e.g. a parent group.

Social networking applications include but are not limited to:

- Blogs
- Any online discussion forums, including professional forums
- Collaborative spaces such as Wikipedia
- Media sharing services e.g. YouTube, Flickr
- 'Microblogging' applications e.g. X

When using school approved social networking sites, the following statements apply: -

- School equipment should not be used for any personal social networking use
- Staff must not accept friendships from underage pupils (18). The legal age for students to register with a social networking site is usually 13 years; be aware that some users may be 13 or younger but have indicated they are older.
- It is important to ensure that members of the public and other users know when a social networking application is being used for official school business. Staff must use only their @xxxxx.dudley.sch.uk email address or other school approved email mechanism and ensure all contributions are professional and uphold the reputation of the school
- Social networking applications should not be used to publish any content which may result in actions for defamation, discrimination, breaches of copyright, data protection or other claims for damages. This includes but is not limited to material of an illegal, sexual or offensive nature that may bring the school into disrepute.
- Postings should not be critical or abusive towards the school, staff, pupils or parents or used to place a pupil, student or vulnerable adult at risk of harm
- The social networking site should not be used for the promotion of personal financial interests, commercial ventures or personal campaigns, or in an abusive or hateful way

- Ensure that the appropriate privacy levels are set. Consider the privacy and safety settings available across all aspects of the service – including photos, blog entries and image galleries. Failing to set appropriate privacy levels could result in messages which are defamatory, libellous or obscene appearing on your profile before you have chance to remove them
- It should not breach the schools Information Security policy

Data Protection

The processing of personal data is governed by the Data Protection Act 2018. Schools are defined in law as separate legal entities for the purposes of complying with the Data Protection Act. Therefore, it is the responsibility of the School, and not the Local Authority, to ensure that compliance is achieved.
As an employee, you should exercise due care when collecting, processing or disclosing any personal data and only process personal data on behalf of the School. The main advantage of the internet and e-mail is that they provide routes to access and disseminate information.

Through your work, personal data will come into your knowledge, possession or control. In relation to such personal data whether you are working at the School*'s* premises or working remotely you must: -

- keep the data private and confidential and you must not disclose information to any other person unless authorised to do so. If in doubt ask your Head Teacher or line manager;
- familiarise yourself with the provisions of the Data Protection Act 2018 and comply with its provisions;
- familiarise yourself with all appropriate school policies and procedures;
- not make personal or other inappropriate remarks about staff, pupils, parents or colleagues on manual files or computer records. The individuals have the right to see all information the School holds on them subject to any exemptions that may apply.
- If you make or encourage another person to make an unauthorised disclosure knowingly or recklessly you may be held criminally liable.

I have read through and fully understand the terms of the policy. I also understand that the school may amend this policy from time to time and that I will be issued with an amended copy.
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:

Appendix 9: 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. The incident log at Hales Valley Trust is via CPOMS.
- 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, the school will follow our retention policy and it will be stored in the main office for access by the Office manager and Senior staff.

Name: ..... Signed: .....

Date:.....

Appendix 10: 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 Harassment

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