Hadley Wood Primary School
Online Safety Policy

Date the policy came into effect	**November 2019**
Date of next policy review	**November 2020**
Name of person responsible for this policy	**Fran Worby**
Issued to	**Staff, governors, parents**
Date of issue	**November 2019**

The purpose of the Online Safety Policy

The purpose of this policy is to ensure that all staff, parents, governors, volunteers and children at Hadley Wood Primary School understand and agree the school's approach to online safety.

Online safety is an integral part of safeguarding and requires a whole school, cross-curricular approach and collaboration between key school leads. Accordingly, this policy is written in line with 'Keeping Children Safe in Education' 2019 (KCSIE), 'Teaching Online Safety in Schools' 2019 and other statutory documents. It complements existing and forthcoming subjects including Health, Relationships and Sex Education, Citizenship and Computing; it is designed to sit alongside our school's statutory Safeguarding Policy. Any issues and concerns with online safety must follow the school's safeguarding and child protection procedures.

Our Online Safety Policy has been written by the school. It has been agreed by the Senior Management Team and approved by the Governing Body in November 2019. This policy is a living document, subject to full annual review but also amended where necessary during the year in response to developments in the school and local area. Although many aspects will be informed by legislation and regulations, staff, governors, pupils and parents will be involved in writing and reviewing the policy. This will help us ensure that all stakeholders understand the rules that are in place. Age-related Acceptable Use Policies (see appendices) support all stakeholders to access the core content of this document.

Key People

Designated Safeguarding Lead (DSL)	Fran Worby
Designated Safeguarding Team	Paula Bertram and Rachael Byrne
Online-safety lead	Fran Worby
Online-safety / Safeguarding Link Governor	Elaine Hayward
PSHE/RSHE lead	Christina Bassilli
Network manager / other technical support	Jill Rose

How will this policy be communicated?

This policy can only impact upon practice if it is a (regularly updated) living document. It must be accessible to and understood by all stakeholders. It will be communicated in the following ways:

- Posted on the school website
- Available on Office 365
- Available in paper format in the staffroom
- Part of school induction pack for all new staff (including temporary, supply and non-classroom-based staff)

- Integral to safeguarding updates and training for all staff (especially in September refreshers)
- Clearly reflected in the Acceptable Use Policies (AUPs) for staff, volunteers, contractors, governors, pupils and parents/carers (which must be in accessible language appropriate to these groups).
- AUPs issued to whole school community, on entry to the school, with annual reminders of where to find them if unchanged, and reissued if updated after annual review
- AUPs are displayed in appropriate classrooms/corridors (not just in Computing corridors/classrooms)
- Reviews of this online-safety policy will include input from staff, pupils and other stakeholders, helping to ensure further engagement

Aims

This policy aims to:

- Set out expectations for all Hadley Wood community members' online behaviour, attitudes, activities and use of digital technology (including when devices are offline)
- Help all stakeholders to recognise that online/digital behaviour standards (including social media activity) must be upheld beyond the confines of the school gates and school day, and regardless of device or platform
- Facilitate the safe, responsible and respectful use of technology to support teaching & learning, increase attainment and prepare children and young people for the risks and opportunities of today's and tomorrow's digital world, to survive and thrive online
- Help school staff working with children to understand their roles and responsibilities to work safely and responsibly with technology and the online world:
    - for the protection and benefit of the children and young people in their care, and
    - for their own protection, minimising misplaced or malicious allegations and to better understand their own standards and practice
    - for the benefit of the school, supporting the school ethos, aims and objectives, and protecting the reputation of the school and profession
- Establish clear structures by which online misdemeanours will be treated, and procedures to follow where there are doubts or concerns (with reference to other school policies such as Behaviour for Learning Policy and Anti-Bullying Policy)

Roles and Responsibilities

Hadley Wood Primary School is a community and all members have a duty to behave respectfully online and offline, to use technology for teaching and learning and to prepare our pupils for life after school. Pupils, parents and staff are to immediately report any concerns or inappropriate behaviour, to protect staff, pupils, families and the reputation of the school. We learn together, make honest mistakes together and support each other in a world that is online and offline at the same time.

The **Headteacher** will:

- Foster a culture of safeguarding where online safety is fully integrated into whole-school safeguarding
- Oversee the activities of the Designated Safeguarding Team and ensure that the DSL responsibilities listed in the section below are being followed and fully supported
- Ensure that policies and procedures are followed by all staff
- Undertake training in offline and online safeguarding, in accordance with statutory guidance
- Liaise with the Designated Safeguarding Team on all online-safety issues which might arise and receive regular updates on school issues and broader policy and practice information
- Take overall responsibility for data management and information security ensuring the school's provision follows best practice in information handling; work with the DPO, DSL and Governing Body to ensure a GDPR-compliant framework for storing data, but helping to ensure that child protection is always put first and data-protection processes support careful and legal sharing of information
- Ensure the school implements and makes effective use of appropriate ICT systems and services including school-safe filtering and monitoring, protected email systems and that all technology including cloud systems are implemented according to child-safety first principles
- Be responsible for ensuring that all staff receive suitable training to carry out their safeguarding and online safety roles
- Understand and make all staff aware of procedures to be followed in the event of a serious online safeguarding incident
- Ensure suitable risk assessments are undertaken so the curriculum meets needs of pupils, including risk of children being radicalised
- Ensure the Governing Body are regularly updated on the nature and effectiveness of the school's arrangements for online safety
- Ensure the school website meets statutory requirements (see appendices for website audit document)

The **Designated Safeguarding Lead / Online Safety Lead** will:

- Take lead responsibility for safeguarding and child protection (including online safety): KCSIE 2019
- Where the Online-Safety Coordinator is not the named DSL or one of the deputy DSLs, ensure there is regular review and open communication between these roles and that the DSL's clear overarching responsibility for online safety is not compromised
- Ensure an effective approach to online safety is adopted to protect and educate the whole community in their use of technology and establish mechanisms to identify, intervene in and escalate any incident where appropriate: KCSIE 2019

- Liaise with the local authority Children's MASH (Multi Agency Safeguarding Hub) and other relevant agencies in line with recommendations outlined in the 'Working Together to Safeguard Children' statutory documentation.
- Take day to day responsibility for online safety issues and be aware of the potential for serious child protection concerns
- Work with the Headteacher, DPO and Governing Body to ensure a GDPR-compliant framework for storing data, but helping to ensure that child protection is always put first and data-protection processes support careful and legal sharing of information
- Stay up to date with the latest trends in online safety
- Review and update this policy, other online safety documents (e.g. Acceptable Use Policies) and the strategy on which they are based (in harmony with policies for Behaviour, Safeguarding, Prevent and others) and submit for review to the Governing Body
- Ensure that online safety education is embedded across the curriculum and beyond, in wider school life
- Promote an awareness and commitment to online safety throughout the school community, with a strong focus on parents
- Liaise with school technical, pastoral, and support staff as appropriate
- Communicate regularly with SLT and the Designated Safeguarding and Online Safety Governor to discuss current issues, review incident logs
- Ensure all staff are aware of the procedures that need to be followed in the event of an online safety incident, and that these are logged in the same way as any other safeguarding incident
- Facilitate training and advice for all staff

The **Governing Body, led by Online Safety / Safeguarding Link Governor** will:

- Approve this policy and strategy and subsequently review its effectiveness
- Ensure an appropriate **senior member** of staff is appointed to the role of DSL with **lead responsibility** for safeguarding and child protection (including online safety)
- Support the school in encouraging parents and the wider community to become engaged in online safety activities
- Have regular strategic reviews with the Online-Safety Co-ordinator / DSL and incorporate online safety into standing discussions of safeguarding at Governing Body meetings
- Where the Online-Safety Coordinator is not the named DSL or one of the deputy DSLs, ensure that there is regular review and open communication between these roles and that the DSL's clear overarching responsibility for online safety is not compromised
- Work with the DPO, DSL and Headteacher to ensure a GDPR-compliant framework for storing data, but helping to ensure that child protection is always put first and data-protection processes support careful and legal sharing of information
- Check all school staff have read Part 1 of KCSIE; SLT and all working directly with children have read Annex A; check that Annex C on Online Safety reflects practice in our school

- Ensure that all staff undergo safeguarding and child protection training (including online safety) at induction. The training should be regularly updated in-line with advice from local safeguarding partners
- Ensure appropriate filters and appropriate monitoring systems are in place. Appropriate care will be taken to ensure that 'overblocking' does not lead to unreasonable restrictions as to what children can be taught with regard to online teaching and safeguarding
- Ensure that children are taught about safeguarding, including online safety as part of providing a broad and balanced curriculum

All **staff** will:

- Understand that online safety is a core part of safeguarding; as such, it is every staff member's responsibility to ensure that statutory guidance is followed
- Know who the Designated Safeguarding Lead (DSL) and Online Safety Lead (OSL) are: **Fran Worby** holds the responsibility of both posts
- Read Part 1, Annex A and Annex C of Keeping Children Safe in Education
- Read and follow this policy in conjunction with the Safeguarding Policy
- Record online-safety incidents in the same way as any safeguarding incident and report in accordance with school procedures
- Understand that safeguarding is often referred to as a jigsaw puzzle – you may have discovered the missing piece so do not keep anything to yourself
- Sign and follow the staff Acceptable Use Policy and Code of Conduct/Staff Handbook
- Notify the DSL/OSL if policy does not reflect practice in our school and follow escalation procedures if concerns are not promptly acted upon
- Identify opportunities to thread online safety through all school activities, both outside the classroom and within the curriculum, supporting curriculum/stage/subject leads, and making the most of unexpected learning opportunities as they arise
- Whenever overseeing the use of technology (devices, the internet, new technology such as augmented reality, etc.) in school or setting as homework tasks, encourage sensible use, monitor what pupils/students are doing and consider potential dangers and the age appropriateness of websites
- Carefully supervise and guide pupils when engaged in learning activities involving online technology (including, extra-curricular and extended school activities if relevant), supporting them with search skills, critical thinking (e.g. fake news), age appropriate materials and signposting, and legal issues such as copyright and data law
- Prepare and check all online source and resources before using within the classroom
- Encourage pupils/students to follow our Acceptable Use Policy, remind them about it at regular intervals and enforce school sanctions
- Notify the DSL/OSL of new trends and issues before they become a problem
- Take a zero-tolerance approach to bullying and low-level sexual harassment
- Be aware that you are often most likely to see or overhear online-safety issues (particularly relating to bullying and sexual harassment and violence) in the

playground, corridors, toilets and other communal areas outside the classroom – let the DSL/OSL know
- Receive regular updates from the DSL/OSL and have a healthy curiosity for online safety issues
- Model safe, responsible and professional behaviours when using technology. This includes outside the school hours and site, and on social media, in all aspects upholding the reputation of the school and of the professional reputation of all staff.

The **PSHE/RSE Curriculum Lead** will:

- Embed consent, mental wellbeing, healthy relationships and staying safe online into the PSHE / Relationships education, relationships and sex education (RSE) and health education curriculum. This will include being taught what positive, healthy and respectful online relationships look like, the effects of their online actions on others and knowing how to recognise and display respectful behaviour online. Throughout these subjects, teachers will address online safety and appropriate behaviour in an age appropriate way that is relevant to their pupils' lives: KCSIE 2019
- Ensure the wider PSHE/RSE curriculum complements the Computing curriculum, which covers the principles of online safety at all key stages, with progression in the content to reflect the different and escalating risks that pupils face.
- Work closely with the DSL/OSL and all other staff to ensure an understanding of the issues, approaches and messaging within PSHE / RSE.

The **Computing Lead** will:

- Oversee the delivery of the online safety element of the Computing curriculum in accordance with the National Curriculum
- Work closely with the DSL/OSL and all other staff to ensure an understanding of the issues, approaches and messaging within Computing
- Collaborate with technical staff and others responsible for ICT use in school to ensure a common and consistent approach, in line with Acceptable-Use Agreements

The **Network Manager/technician** will:

- Keep up to date with the school's online safety policy and technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- Work closely with the Designated Safeguarding Lead / Online Safety Lead / Data Protection Officer to ensure that school systems and networks reflect school policy
- Ensure the above stakeholders understand the consequences of existing services and of any changes to these systems (especially in terms of access to personal and sensitive records / data and to systems such as YouTube mode, web filtering settings, sharing permissions for files on cloud platforms etc
- Support and advise on the implementation of 'appropriate filtering and monitoring' as decided by the DSL and Senior Leadership Team

- Maintain up-to-date documentation of the school's online security and technical procedures
- Report online-safety related issues that come to their attention in line with school policy
- Manage the school's systems, networks and devices, according to a strict password policy, with systems in place for detection of misuse and malicious attack, with adequate protection, encryption and backup for data, including disaster recovery plans, and auditable access controls
- Monitor the use of school technology, online platforms and social media presence and report any misuse/attempted misuse is identified and reported in line with school policy

Work with the Headteacher to ensure the school website meets statutory DfE requirements (see appendices for website audit document

All **Volunteers and Contractors** will:

- Read, understand, sign and adhere to an acceptable use policy (AUP)
- Report any concerns, no matter how small, to the Designated Safety Lead / Online Safety Coordinator as named in the AUP
- Maintain an awareness of current online safety issues and guidance
- Model safe, responsible and professional behaviours in their own use of technology

All **Pupils** will:

- Read, understand, sign and adhere to the student/pupil Acceptable Use Policy and review this annually
- Understand the importance of reporting abuse, misuse or access to inappropriate materials
- Know what action to take if they or someone they know feels worried or vulnerable when using online technology
- Understand the importance of adopting safe and responsible behaviours and good online safety practice when using digital technologies outside of school and realise that the school's Acceptable Use Policy covers actions out of school, including on social media
- Understand the benefits/opportunities and risks/dangers of the online world and know who to talk to at school or outside school if there are problems

All **Parents/Carers** will:

- Read, sign and promote the school's parental Acceptable Use Policy (AUP) and read the pupil AUP and encourage their children to follow it
- Consult with the school if they have any concerns about their children's and others' use of technology
- Promote positive online safety and model safe, responsible and positive behaviours in their own use of technology, including on social media: not sharing other's images or details without permission and refraining from posting negative, threatening or

violent comments about others, including the school staff, volunteers, governors, contractors, pupils or other parents/carers.

Education and Curriculum

The following subjects have the clearest online safety links *(see the relevant role descriptors above for more information):*

- PSHE
- Relationships education, relationships and sex education (RSE) and health
- Computing
- Citizenship

However, as stated in the role descriptors above, it is the role of all staff to identify opportunities to thread online safety through all school activities, both outside the classroom and within the curriculum, supporting curriculum/stage/subject leads, and making the most of unexpected learning opportunities as they arise (which have a unique value for pupils)

At Hadley Wood, we recognise that online safety and broader digital resilience must be thread throughout the curriculum and that is why we are working to adopt the cross-curricular framework 'Education for a Connected World' from UKCIS (the UK Council for Internet Safety).

Teaching and Learning

Why Internet use is important

- The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide children with quality Internet access as part of their learning experience
- Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils

Internet use will enhance learning

- The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of the children
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives / rules for Internet use
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation

Pupils will be taught how to evaluate the Internet content

- The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law
- Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy

Introducing the Online Policy to pupils

- Online Safety rules will be discussed with the pupils at the start of each year and in line with the units set out in the Computing Scheme of Work
- Online safety posters will be posted close to all computers within the classroom and be prominent in environments such as the Media Suite, so all users can see them
- Pupils are informed that network and Internet use is monitored and appropriately followed up
- The children receive regular online safety lessons and are constantly reminded to stay safe online
- Children will be made aware of the Acceptable Use Policy- adapted for KS1 and KS2 (see appendices)
- The school recognises the additional risks that children with SEN and disabilities (SEND) face online (for example from online bullying, grooming and radicalisation) and will put suitable scaffolding into place to ensure that SEND children are able to stay safe online as outlined in the updated KCSIE 2019 documentation

Managing Internet Access

Authorised Internet Access

- All staff must read and sign the 'Acceptable Use Policy' which covers both school use and social networking protocols

World Wide Web

- If staff or pupils discover unsuitable sites, the URL (address), time, content must be reported to the school office, the Online Safety Lead or other senior member of staff, who will then contact the LGFL (our internet provider)
- Pupils should be taught to be critically aware of the materials they are shown and how to validate information before accepting its accuracy
- Pupils should be taught to understand intellectual property rights

Email

- Pupils may not use email in the school
- Pupils and or staff must immediately tell a member of SLT if they receive/gain access to offensive online materials or images online
- All staff must send email communication to parents via the school office. Personal emails to parents are not permitted
- All communication amongst staff using the school email account will be sent within school working hours Monday – Friday to enable a work/life balance is achieved
- Access in school to external personal e-mail accounts may be blocked
- E-mail sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on school headed paper
- The forwarding of chain letters is not permitted

School Website

- The contact details on the school website should be the school address, email and telephone number.

- Staff or pupils' personal information will not be published
- The Office Manager, Headteacher or nominee will take overall editorial responsibility and ensure that content is accurate and appropriate.
- Photographs that include pupils will be selected carefully
- Pupils' names will not be used anywhere on the website, particularly in association with photographs
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website
- Parents of new pupils will be made aware of our policy on the usage of digital images of children
- Pupil's work can only be published on the school website where parents have given permission. Work will not be published where the parent/carer has refused permission

Social Networking

- Social media is a fact of modern life, and as a school, we accept that many parents, staff and pupils will use it. However, as stated in the Acceptable Use Policies which all members of the school community sign, we expect everybody to behave in a positive manner, engaging respectfully with the school and each other on social media, in the same way as they would face to face.
- This positive behaviour can be summarised as not making any posts which are or could be construed as bullying, aggressive, rude, insulting, illegal or otherwise inappropriate, or which might bring the school or (particularly for staff) teaching profession into disrepute. This applies both to public pages and to private posts, e.g. parent chats, pages or groups.
- If parents have a concern about the school, we would urge them to contact us directly and in private to resolve the matter. If an issue cannot be resolved in this way, the school complaints procedure, available on our website, should be followed. Sharing complaints on social media is unlikely to help resolve the matter, but can cause upset to staff, pupils and parents, also undermining staff morale and the reputation of the school (which is important for the pupils we serve).
- The school will deny access to social networking sites and newsgroups unless a specific use is approved. Children will be strongly advised not to use these at home in line with the Terms of Use linked to each service. Reminders will be shared with parents through the school newsletter and Parent Online Safety Information Sessions delivered by a CEOP accredited trainer
- Pupils will be advised never to give out personal details of any kind which may identify them or their location
- Pupils will be advised not to place personal photos on any social network space in their termly online safety lessons
- Pupils will be informed of the importance of not sharing pictures online (of a sexual, naked or semi-naked image or video of themselves) or send sexually explicit messages (sexting) in line with KCSIE 2019 recommendations
- Pupils will be informed about 'online bullying' as a form of peer on peer abuse which involves sending inappropriate or hurtful text messages, emails or instant messages and of the appropriate action they would need to take
- Pupils will be educated on the importance of not sending offensive messages, posting malicious material online (e.g. on social networking websites) or sending or posting offensive or degrading images and videos;

- Pupils will be advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications. Pupils should be encouraged to invite known friends only and deny access to others

Filtering

The school will work in partnership with the Local Authority, Becta and the Internet Service Provider to ensure filtering systems are as effective as possible

Video Conferencing

- IP videoconferencing should use the educational broadband network to ensure quality of service and security rather than the Internet
- Pupils should ask permission from the supervising teacher before making or answering a videoconference call
- Videoconferencing will be appropriately supervised for the pupils' age

Managing Emerging Technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed
- Mobile phones will not be used for personal use during school time. The sending of abusive or inappropriate text messages is forbidden

Personal devices including wearable technology and bring your own device (BYOD)

- Pupils in Years 5 and 6 who walk home alone are allowed to bring mobile phones in for emergency use only, but not when moving around the school buildings. During lessons, phones must remain turned off at all times and kept in their school bag. Any attempt to use a phone in lessons without permission or to take illicit photographs or videos will lead to an immediate Stage 3 sanction and the withdrawal of mobile privileges. Important messages and phone calls to or from parents can be made at the school office, which will also pass on messages from parents to pupils in emergencies.
- All staff who work directly with children should leave their mobile phones on silent and only use them in private staff areas during school hours.
- Child/staff data should never be downloaded onto a private phone. If a staff member is expecting an important personal call when teaching or otherwise on duty, they may leave their phone with the school office to answer on their behalf or ask for the message to be left with the school office.
- Volunteers, contractors, governors should leave their phones in their pockets and turned off. Under no circumstances should they be used in the presence of children or to take photographs or videos. If this is required (e.g. for contractors to take photos of equipment or buildings), permission of the Headteacher should be sought and this should be done in the presence of a member of staff.
- Parents are asked to leave their phones in their pockets and turned off when they are on site. They should ask permission before taking any photos, e.g. of displays in corridors or classrooms, and avoid capturing other children. When at school events, Parents are asked not to post photographs taken on social media sites. Parents are

asked not to call pupils on their mobile phones during the school day; urgent messages can be passed via the school office.

Information System Security

- School ICT systems capacity and security will be reviewed regularly
- Virus protection is installed and automatically updated
- Security strategies will be discussed with the Local Authority

Protecting Personal Data

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018. Any concerns relating to the schools handling of data should be conveyed to the borough appointed Data Protection Officer (DPO).

Searching and confiscation

In line with the DfE guidance 'Searching, screening and confiscation: advice for schools', the Headteacher and staff authorised by them have a statutory power to search pupils/property on school premises. This includes the content of mobile phones and other devices, for example as a result of a reasonable suspicion that a device contains illegal or undesirable material, including but not exclusive to sexual images, pornography, violence or bullying. Full details of the school's search procedures are available in the school Behaviour Policy

Handling online-safety concerns and incidents

It is vital that all staff recognise that online-safety is a part of safeguarding (as well as being a curriculum strand of Computing, PSHE/RSHE and Citizenship.

General concerns must be handled in the same way as any other safeguarding concern; safeguarding is often referred to as a jigsaw puzzle, so all stakeholders should err on the side of talking to the Online-Safety Lead / Designated Safeguarding lead to contribute to the overall picture or highlight what might not yet be a problem.

Support staff will often have a unique insight and opportunity to find out about issues first in the playground, corridors, toilets and other communal areas outside the classroom (particularly relating to bullying and sexual harassment and violence).

School procedures for dealing with online-safety will be mostly detailed in the following policies (primarily in the first key document):

- Safeguarding and Child Protection Policy
- Anti-Bullying Policy
- Behaviour for Learning Policy
- Acceptable Use Policies
- Data Protection Policy

This school commits to take all reasonable precautions to ensure online safety, but recognises that incidents will occur both inside school and outside school (and that those from outside school will continue to impact on pupils when they come into school. All

members of the school are encouraged to report issues swiftly to allow us to deal with them quickly and sensitively through the school's escalation processes.

Any suspected online risk or infringement should be reported to the Online Safety Lead / Designated Safeguarding Lead on the same day – where clearly urgent, it will be made by the end of the lesson.

Any concern/allegation about staff misuse is always referred directly to the Headteacher, unless the concern is about the Headteacher in which case the compliant is referred to the Chair of Governors and the LADO (Local Authority's Designated Officer). Staff may also use the NSPCC Whistleblowing Helpline

The school will actively seek support from other agencies as needed (i.e. the local authority, LGfL, UK Safer Internet Centre's Professionals' Online Safety Helpline, NCA CEOP, Prevent Officer, Police, IWF). We will inform parents/carers of online-safety incidents involving their children, and the Police where staff or pupils engage in or are subject to behaviour which we consider is particularly disturbing or breaks the law.

Review

The policy will be reviewed at least every year, or as new guidance becomes available to schools from Department of Education (DfE)

Hadley Wood Acceptable Use Policy: KS1 Children

	# Think before you click!
S 	**I will only use devices or apps, sites or games if a trusted adult says so**
A 	**I know people online aren't always who they say they are**
F 	**I will only send friendly and polite messages. I know that anything I do online can be shared and might stay online forever**

E 	**If I see something I don't like on a screen, I will always tell an adult**

With the help of my teacher I have read and understand these rules. I will try my best to follow them.

Signed: ***Date:***

Hadley Wood Acceptable Use Policy: KS2 Children

For my own personal safety:

- I will treat my username and password like my toothbrush – I will not share it, nor will I try to use any other person's username and password.
- I am aware that some websites and social networks have age restrictions and I should respect this.
- I only use the devices, apps, sites and games - whether at home or school- when I am allowed to, at the times I am allowed to.
- I will only e-mail people I know, or a responsible adult has approved.
- I will be aware of "stranger danger", when I am communicating on-line.
- I will not give my home address, phone number, send a photograph or video, or give any other personal information that could be used to identify me, my family or my friends, unless a trusted adult has given permission.
- I will never arrange to meet someone I have only ever previously met on the Internet, unless my parent/carer has given me permission and I take a responsible adult with me.
- I will talk to a trusted adult if anything upsets me or worries me on an app, site or game – it often helps. If I get a funny feeling, I talk about it.
- I know it's not my fault if I see or someone sends me something bad – I won't get in trouble, but I mustn't share it. Instead, I will tell a trusted adult. If I make a mistake, I don't try to hide it but ask for help.
- I will not do live videos (livestreams) on my own – and always check if it is allowed. I check with a trusted adult before I video chat with anybody for the first time.
- I keep my body to myself online – I never get changed or show what's under my clothes in front of a camera. I remember my body is mine and no-one should tell me what to do with it; I don't send any photos or videos without checking with a trusted adult.
- I will hand in my mobile phone to the office each morning.
- I say no online if I need to – I don't have to do something just because a friend dares or challenges me to do it, or to keep a secret. If I get asked anything that makes me worried, upset or just confused, I should say no, stop chatting and tell a trusted adult immediately.

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

- I won't share anything that I know another person wouldn't want shared, or which might upset them. And if I know a friend is worried or needs help, I will remind them to talk to an adult, or even do it for them.
- I understand that nasty/hurtful messages would be considered as online bullying.
- I am not a bully – I do not post, make or share unkind, hurtful or rude messages/comments and if I see it happening, I will tell my trusted adults.
- I will not take or distribute images of anyone without their permission.
- I will only edit or delete my own files and not look at, or change, other people's files without their permission.
- I am careful what I share and protect my online reputation – I know anything I do can be shared and might stay online forever (even on Snapchat or if I delete it).
-

When using the internet for research:

- I will only use other people's writing, pictures, music or video if I know I have copyright permission.
- I use safe search tools approved by my trusted adults. I know I can't believe everything I see online, know which sites to trust, and know how to double check information I find.

Keeping our school system secure:

- I understand that the school will monitor my use of the ICT systems, email and other digital communications.
- I will not click on unexpected links or popups, and only download or install things when I know it is safe or has been agreed by trusted adults. Sometimes add-ons can cost money, so it is important I always check for these too
- I will not attempt to visit Internet sites that I know to be banned by the school.
- I will only use the school's computers for schoolwork and homework.
- I will not bring files into school without permission or upload inappropriate material to my workspace.

I have read and understand these rules and agree to them.

Signed: ***Date:***