Pupil Acceptable Use of Technology Statements

Early Years and Key Stage 1 (0-6)

- I understand that the school rules will help keep me safe and happy when I go online.
- I only go online when an adult is with me.
- I check with an adult before I click on links or things online.
- I keep my personal information and passwords safe.
- I only send polite and friendly messages online.
- I know the school can see what I am doing online when I use school computers and tablets including if I use them at home.
- If I see something online that makes me feel upset, unhappy, or worried, I will always tell an adult.
- I can visit www.ceopeducation.co.uk to learn more about keeping safe online.
- I know that if I do not follow the school rules:
    - I will be given appropriate sanctions;
    - My parents/carers may be notified;
    - I may have to be supervised more closely when using technology in school (if applicable).
- I have read and talked about these rules with my parents/carers.

Shortened KS1 version (for use on posters or with very young children)

- I only go online with a grown-up.
- I am kind online.
- I keep information about me safe online.
- I tell a grown-up if something online makes me unhappy or worried.

Key Stage 2 (7-11)

I understand that the school Acceptable Use Policy will help keep me safe and happy online at home and at school.

Safe

- I will be kind and respectful online, just like I am in school.
- I will only share pictures or videos online if they are safe, kind, and I have asked for permission first.
- I will only click on links if I know what they do, or I will ask a safe adult first.
- I will only chat with people I know online, or I will ask a safe adult to help me decide if someone I don't know is safe to speak with online.
- If someone online asks to meet me, I will tell a safe adult straight away.

Learning

- I follow the school rules about mobile phones and smart technology.
- I always ask permission from an adult before using the internet.
- I only use websites, tools and/or search engines that an adult has chosen or given me permission to use.
    - I must always add 'for kids' or 'for children' after anything I google to ensure the content is appropriate.
- I use school devices for school work unless I have been told otherwise.
- If I need to learn online at home, I will follow the same rules in this policy

Trust

- I know that some things or people online might not be honest or truthful.
- If I'm unsure if something online is true, I will check other websites, books, or ask a safe adult.
- I always credit the person or source that created any work, images, or text I use.
- I will only use Artificial Intelligence (AI) tools when an adult says it is allowed.
- I will not put personal information about me or anyone else into AI tools. I will not use AI to make fake images, voices, videos or messages about other people.

Responsible

- I keep my personal information safe and private online.
- I will keep my passwords safe and will not share them.
- I will not access or change other people's files or information.
- I will only change the settings on a device if a member of staff has allowed me to.

Tell

- If I see anything online that makes me feel worried, upset, or frightened, I will tell an adult straight away, I will not click or open any links before I alert an adult.
- If I am aware of anyone being unkind or unsafe with technology, I will report it to an adult.
- If an AI tool shows me something worrying, unkind, rude, violent, confusing or unsafe, I will stop and tell a safe adult.
- I understand that the adults at school are responsible for keeping me safe; they may need to speak to other safe adults, or my parents/carers, if I tell them about something that has happened online.
- I can visit www.ceopeducation.co.uk and www.childline.org.uk to learn more about being safe online or to seek help.

Understand

- I understand that the school internet filter is there to protect me, and I will not try to bypass it.
- I know that all school owned devices and networks are checked/monitored to help keep me safe, even if I use them at home. This means someone at the school may be able to see and/or check my online activity when I use school devices and networks if they are worried about my or anyone else's safety or behaviour.
- If I bring a mobile phone or other device to school (only with permission and in exceptional circumstances, I will follow the rules. I know that it is to be handed into the office and then collected at the end of the school day. I will not use it during the school day unless a member of staff has agreed this.
- I understand that my behaviour online can affect others and I will not behave in a way that will upset, frighten or embarrass others.
- I have read and talked about these rules with my parents/carers.
- I know that if I do not follow the school rules then:
    - I will be given an appropriate sanction/s.

Alternative KS2 Statements

- I understand that the school Acceptable Use Policy will help keep me safe and happy online at home and at school.
- I know that I will be able to use the internet in school for a variety of reasons, if I use it responsibly. However, I understand that if I do not, I may not be allowed to use the internet at school.
- I know that being responsible means that I should not look for bad language, inappropriate images or violent or unsuitable games, and that if I accidentally come across any of these, I should report it to a teacher or adult in school or a parent or carer at home.
- I will treat my password like my toothbrush! This means I will not share it with anyone (even my best friend), and I will log off when I have finished using the computer or device.

- I will protect myself by not telling anyone online my address, my telephone number, my school or by sending a picture of myself without permission from a safe adult.
- I will not arrange to meet anyone I have met online alone in person without talking to a safe adult first.
- I will only use AI tools when my teacher or another safe adult says it is allowed. I will not put personal information about me or anyone else into AI tools. I will not use AI to make fake images, voices, videos or messages about other people. If an AI tool shows me something worrying, unkind, rude, violent, confusing or unsafe, I will stop and tell a safe adult.
- If I get unpleasant, rude, or bullying emails or messages, I will report them to a teacher or other adult. I will not delete them straight away, but instead, keep them so I can show them to the person I am reporting it to.
- I will always be myself and not pretend to be anyone or anything I am not. I know that posting anonymous messages or pretending to be someone else is not allowed.
- I will always check before I download software or data from the internet. I know that information on the internet may not be reliable, and it sometimes needs checking.
- If I bring in memory sticks/CDs from outside of school I will always give them to my teacher so they can be checked for viruses and content before opening them.
- I will be polite and sensible when I message people online and I know that sending a message is the same as having a conversation with someone. I will not be rude or hurt someone's feelings online.
- I know that I am not allowed on personal email, social networking sites or instant messaging in school.
- If, for any reason, I need to bring a personal smart device and/or mobile phone into school I know that it is to be handed in to the office and then collected at the end of the school day.
- I know that my use of school provided devices, accounts and systems may be monitored to help keep people and systems safe, including when I use them away from the school.
- I will tell a teacher or other adult if someone online makes me feel uncomfortable or worried when I am online using games or other websites or apps.

Shortened KS2 version (for use on posters)

- I ask an adult about which websites I can use.
- I will not assume information online is true.
- I know there are laws that stop me copying online content.
- I know I must only open online messages that are safe. If I am unsure, I will not open it without speaking to an adult first.
- I know that people online are strangers, and they may not always be who they say they are.
- If someone online suggests meeting up, I will always talk to an adult straight away.
- I will not use technology to be unkind to people.
- I will keep information about me and my passwords private.
- I always talk to an adult if something which makes me feel worried.
- I know my use of school devices and systems can be monitored.

Pupils with Special Educational Needs and Disabilities (SEND)

Learners with SEND functioning at Levels P4 –P7

- I only use phones, tablets or computers when a grown-up says it is okay.
- I make good choices on the computer.
- I use kind words on the internet.
- I tell a grown-up if I see or hear something online that upsets me.
- I know that if I do not follow the school rules then:
    - I will be given appropriate sanctions.

Learners with SEND functioning at Levels P7-L1 (Based on Childnet's SMART Rules)

Safe

- I ask a grown up if I want to use a phone, tablet or computer.
- I do not tell strangers my name on the internet.
- I know that if I do not follow the school rules then:
    - I will be given appropriate sanctions.

Meeting

- I tell a grown-up if I want to talk on the internet.

Accepting

- I do not open messages or emails from strangers.

Reliable

- I make good choices on the computer.

Tell

- I use kind words on the internet.
- If I see anything online that worries me, I will tell a grown up.

Learners with SEND functioning at Levels L2-4 (Based on Childnet's SMART Rules)

Safe

- I ask an adult if I want to use the internet.
- I use phones, tablets or computers when an adult says it is okay.
- I keep my information private on the internet.
- I ask an adult before I take or share a photo, video or message.

- I know that if I do not follow the school rules then:
  - I will be given appropriate sanctions

Meeting

- I tell an adult if I want to talk to people on the internet.
- If I meet someone online, I talk to an adult.

Accepting

- I do not open messages from strangers.
- I check web links to make sure they are safe.

Reliable

- I make good choices on the internet.
- I check the information I see online.

Tell

- I use kind words on the internet.
- If someone is mean online, then I will not reply. I will save the message and show an adult.
- If I see anything online that worries or upsets me, I will tell a teacher.

Optional additional SEND statements: mobile phones, devices and AI

Mobile phones, smart technology and personal devices

- I only use phones, tablets, computers or devices when a grown-up says it is okay.
- I ask a grown-up before I use a phone, tablet, camera or device.
- I follow the school rules about phones, tablets, cameras and smart devices.
- If I bring a phone or device to school I only use it when a member of staff says I can
- I keep my phone or device where the school says it should be.
- I follow the school rules about where my phone or device should be kept. This means:
- I ask before I look at, touch or use someone else's device.
- I do not use a phone, camera or device to take photos, videos or recordings unless a member of staff says this is okay.
- I do not send or share photos, videos, messages or recordings without permission.
- I use kind words when I send messages.
- If I see or hear something I do not like on a device, I tell a grown-up.
- If I receive a message, image or video that worries me, I will tell a safe adult.
- If someone asks me to share a photo, video or personal information, I will ask a safe adult for help.
- I ask for help if I am not sure what to do on a device.

Agreed device use for individual needs

- If I use a phone or device to help with my health, communication or support needs, I will use it in the way staff have explained.
- I will only use my device for the specific reason it has been provided or allowed.
- I will not use my device to take photos, record, send messages or go online unless staff have said this is part of my support plan.
- If I need help using my device safely, I will ask a safe adult.
- I understand that having permission to use a device does not mean I can use it for anything I want during the school day.

Artificial intelligence

- AI means technology that can make or suggest things, like words, pictures, videos, voices, answers or ideas. I will only use AI when an adult says I can.
- I use AI with help from an adult.
- I ask an adult before I use AI.
- I will only use AI tools that the school has said I can use.
- I will only use AI tools in the way staff have shown me.
- I do not put information about me into AI.
- I do not put information about other people into AI.
- I will not put names, photos, personal information or private information about me or other people into AI tools.
- I do not use AI to pretend to be someone else.
- I do not use AI to make fake pictures, voices, videos or messages about people.
- I do not use AI to make anything unkind or upsetting about another person.
- I know that AI can make mistakes, so I will check information with an adult.
- If AI shows me something worrying, unsafe, unkind or confusing, I will stop and tell an adult.
- I understand that AI can help me learn, but it should not do all my work for me.
- I will ask for help if I am not sure whether I can use AI for my work.

Wider safe technology use

- I ask an adult before I use technology.
- I use technology in the way adults have agreed.
- I follow the school rules for phones, devices, cameras, computers and AI tools.
- I tell an adult if something online or on a device makes me worried.
- I do not use technology to upset, trick or hurt other people.
- I ask an adult before I share information, pictures or videos.
- I know adults at school can help me use technology safely.

Pupil Acceptable Use Policy Agreement Form

Hollingbourne Primary School Acceptable Use of Technology Policy – Pupil Agreement

I, with my parents/carers, have read and understood the school] Acceptable Use of Technology Policy (AUP).

I agree to follow the AUP when:

1. I use school devices and systems, both on site and at home.
2. I bring my own devices into school including mobile phones, smart technology, gaming devices, cameras, or any device that can send or receive messages or notifications, or record audio, images or video.
3. I use my own systems or equipment outside of school including when communicating with other members of the school or when accessing school systems.

Name……. Signed…….……..….

Class…….…… Date…….

Parent/Carer's Name……..…….....

Parent/Carer's Signature…….……

Date………

Acceptable Use of Technology Sample Statements and Forms for Parents/Carers

Parent/Carer AUP Acknowledgement Form

Hollingbourne Primary School Acceptable Use of Technology Policy Acknowledgement

1. I have received and read the Hollingbourne Primary School pupil Acceptable Use of Technology Policy (AUP) and have discussed its expectations with my child in a way that is appropriate to their age, understanding and needs.

2. I understand that the AUP explains how my child is expected to use technology safely, kindly, lawfully and responsibly, including when using:
    - School provided devices, accounts, systems and internet access;
    - School provided technology away from the setting;
    - personal devices or services where their use affects the safety or wellbeing of a child or another person, disrupts the safe or effective operation of the school or raises a safeguarding or behaviour concern.

3. I understand that access to online content through school devices and systems is appropriately filtered and that use of school provided devices, accounts and systems may be monitored, including when they are used away from the setting. The school has provided information about its filtering and monitoring arrangements.
4. I understand that filtering and monitoring arrangements help to keep children safe, protect systems and support compliance with relevant policies, but cannot remove every online risk. Monitoring will be proportionate and undertaken in accordance with data protection, privacy and human rights requirements.

5. I am aware of the school's expectations concerning mobile phones and smart devices and will support my child to follow them. If my child may need an exception or reasonable adjustment because of a disability, medical condition, communication need or other individual circumstance, I will discuss this with the school so that appropriate arrangements can be considered, agreed and recorded. I will support any individual arrangements agreed for my child. If I need to contact my child during the school day, I will use the school office or another agreed contact route, unless an alternative arrangement has been agreed.

6. I will support my child to understand and follow the school's expectations for technology use, including social media, mobile phones, online communication, images and recordings and, where relevant, artificial intelligence tools.

7. I will model safe, positive and respectful online behaviour and support my child not to create, post or share content that identifies, targets, threatens, bullies, harasses or risks causing harm to a child, family, member of staff or another member of the school

community.

8. If I have a concern or complaint, I am encouraged to use the school's established communication, safeguarding or complaints routes, as appropriate, so that it can be properly considered.

9. I will report concerns about my child's online safety, or online concerns that may affect the safety or wellbeing of another member of the school community, to an appropriate member of staff. This may include the class teacher, the Designated Safeguarding Lead or headteacher. Where necessary, I may also report the concern to another relevant organisation.

10. If the school has concerns about my child's online safety or behaviour, I understand that these will be considered fairly and proportionately in line with relevant safeguarding, behaviour and other procedures. The school will communicate with me where it is appropriate and safe to do so.

11. I understand my role in helping my child to use technology safely. As appropriate to my child's age, understanding and needs, I will consider the use of parental controls, provide suitable supervision and support, and encourage safe and responsible use of the internet and other technology at home.

12. I know that I can seek online safety information or support from the school by speaking with relevant staff, such as my child's class teacher, the headteacher, the Designated Safeguarding Lead or by going onto the school website for help and advice.

I acknowledge that I have received and read the Hollingbourne Primary School pupil Acceptable Use of Technology Policy and have discussed its expectations with my child.

Child's name: .....

Class/group: .....

Child's signature: .....

Parent/carer's name: .....

Parent/carer's signature: .....

Date: .....

Sample Parent/Carer Acceptable Use of Technology Policy (AUP)

1. Access to technology

I understand that my child will be provided with internet access and may use a range of technology, devices, accounts and online services at Hollingbourne Primary School, to support their learning, development and preparation for life in a digital world.

2. Scope of the pupil AUP

I understand that the pupil AUP applies to my child's use of school-provided devices, accounts, systems and internet access, both on site and when accessed away from the school

Relevant school expectations may also apply to personal technology use where online behaviour:

- affects the safety or wellbeing of a child, member of staff or another person;
- disrupts the safe or effective operation of the school or
- raises a safeguarding, behaviour or potentially unlawful concern.

3. Understanding the pupil AUP

I have received and read the Hollingbourne Primary School Pupil Acceptable Use of Technology Policy and have discussed its expectations with my child in a way that is appropriate to their age, understanding and needs.

4. Supporting safe and responsible technology use

I will support my child to understand and follow the school's expectations for safe, kind, lawful and responsible use of technology. This includes expectations relating to online communication, social media, images and recordings and, where relevant, artificial intelligence tools.

I understand that guidance, legislation, technology and online risks may change and that the school may review and update its policies and expectations in response.

5. Mobile phones and smart technology

I am aware that the school has clear expectations concerning children's use of mobile phones and smart technology.

In schools, pupils should not use, access, display or check mobile phones or similar smart technology during the school day, including during lessons, time between lessons, breaktimes and lunchtime, unless a specific exception or reasonable adjustment has been agreed.

Where my child may need access to a mobile phone or smart device because of a disability, medical condition, communication need or other individual circumstance, I will discuss this with the school Any exception or reasonable adjustment will be considered individually and, where agreed, the purpose, arrangements and expectations for use will be clearly recorded and communicated to my child and relevant staff.

I will support the school's expectations and any individual arrangements agreed for my child. I will not contact my child directly on their mobile phone or smart device during the school day unless this forms part of an agreed arrangement. If I need to contact my child during the day, I will use the school office or another agreed contact route.

6. Filtering

I understand that access to online content through school provided devices, systems and internet services is appropriately filtered. Information about the filtering arrangements in place is available.

7. Monitoring

I am aware that my child's use of school-provided devices, accounts and systems may be monitored, including when those devices, accounts or systems are used away from the school Information about the monitoring arrangements in place is available.

Monitoring is used to help keep children safe, protect systems and check compliance with relevant policies. It will be proportionate and undertaken in accordance with data protection, privacy and human rights requirements.

8. Limitations of filtering and monitoring

I understand that the school will take reasonable and proportionate steps, including the use of appropriate filtering and monitoring arrangements, to help keep children safe when using school-provided devices and systems.

I understand that no filtering or monitoring system can remove every online risk, particularly where online content changes rapidly or where children use personal devices, accounts, networks or services outside the school's systems.

9. Online safety education

I understand that my child will receive age and ability-appropriate online safety education to help them use technology safely and responsibly, both within and outside the school

I recognise that education, appropriate supervision, open communication and opportunities to seek help remain important alongside technical measures such as filtering and monitoring.

10. Supporting my child at home

I understand my role in helping my child to use technology safely. As appropriate to my child's age, understanding and needs, I will:

- consider the use of suitable parental controls and safety settings;
- provide appropriate supervision, support and guidance;
- talk to my child about their online experiences;
- encourage safe, kind, lawful and responsible online behaviour; and
- help my child understand how and where to seek support.

11. Remote and online learning

Where my child accesses remote or online learning, I will support them to follow the school's remote/online learning expectations. I will help my child to access learning from an appropriate location and provide supervision and support that reflects their age, understanding and needs.

I understand that the school will provide information about the systems and sites my child is expected to access and who from the school if anyone, they will interact with online.

12. Positive and respectful online behaviour

I will support the school's approach to online safety and model safe, positive and respectful online behaviour, including when creating or sharing images, text, audio or video.

I will support my child not to create, post or share content that identifies, targets, threatens, bullies, harasses or risks causing harm to a child, family, member of staff or another member of the school community.

13. Raising concerns and complaints

If I have a concern or complaint, I am encouraged to use the school's established communication, safeguarding or complaints routes, as appropriate, so that the matter can be properly understood and considered.

Information about how to raise a concern, safeguarding report or complaint is available.

I will report concerns about my child's online safety, or online concerns that may affect the safety or wellbeing of another member of the school community, to an appropriate member of staff.

This may include:

- Class teacher
- the Designated Safeguarding Lead (Mrs Allen-Harding)
- the headteacher

Where necessary, I may also report the concern to another relevant organisation or emergency service.

14. Responding to online concerns

If the school has concerns about my child's online safety, online behaviour or use of technology, I understand that these will be considered fairly and proportionately under the setting's child protection, behaviour and other relevant policies.

The school may also need to consider an appropriate response where online behaviour involving a parent/carer affects the safety or wellbeing of a child, member of staff or another person; disrupts the safe or effective operation of the school involves confidential or personal information; or raises a safeguarding or potentially unlawful concern. Any such concern will be considered fairly and proportionately, taking account of the particular circumstances and in line with the school's complaints policy or other relevant arrangements.

The school will communicate with those involved where it is appropriate and safe to do so. I understand that there may be circumstances in which the setting must first follow its safeguarding

procedures or seek advice from another agency. Where behaviour may be unlawful or presents a risk to safety, the school may seek appropriate safeguarding, police or legal advice.

15. Online safety advice and support

I know that I can seek information or support from the school about online safety and helping my child to use technology safely. Information is available through the school website or online.

16. Agreement

I confirm that I have read and understood the school's Parent/Carer Acceptable Use of Technology Policy and agree to support its expectations and the safe, lawful and responsible use of technology by my child.

Child's name: .....

Class/group: .....

Child's signature: .....

Parent/carer's name: .....

Parent/carer's signature: .....

Date: .....

Acceptable Use of Technology for Staff, Visitors and Volunteers Sample Statements

Staff Acceptable Use of Technology Policy (AUP)

As a professional organisation with responsibility for safeguarding, all staff are expected to use technology in a professional, lawful, ethical and responsible manner.

This Staff Acceptable Use of Technology Policy (AUP) sets out school expectations for safe technology use, professional conduct, safeguarding, data protection and system security. It is not intended to unduly limit appropriate teaching, learning or professional use of technology, but to help protect pupils, staff, systems and the wider school community from accidental or deliberate misuse.

All staff are asked to read, understand and sign this AUP.

Policy scope

1. I understand that this policy applies to my use of technology systems and services provided by the school or accessed by me as part of my role within Hollingbourne Primary School, both on and offsite. It also applies to personal use of technology where this is linked to my role, involves the school community, uses school systems or information, could affect safeguarding, professional boundaries, confidentiality or data protection, or could reasonably impact on my professional role or the reputation of the school.

2. I understand that Hollingbourne Primary School Acceptable Use of Technology Policy (AUP) should be read and followed in line with the school child protection policy and staff code of conduct.

3. I am aware that all staff should ensure that technology use is consistent with the school ethos, school staff behaviour and safeguarding policies, national and local education and child protection guidance, and the law.

Use of school devices and systems

4. I will use school-provided or approved equipment, systems and internet services when working with pupils, unless otherwise formally agreed by leaders.

5. I understand that school equipment, systems and internet services are provided for education and/or professional use. Reasonable personal use is not permitted and, where allowed, must not interfere with my work duties, system security, safeguarding, confidentiality or professional boundaries. This permission is at the school's discretion and may be withdrawn at any time.

6. Where I deliver or support remote/online learning, I will comply with the school remote/online learning AUP.

Data and system security

7. To prevent unauthorised access to systems or personal data, I will not leave any information system unattended without first logging out or securing/locking access.
    - I will follow the school's requirements for secure passwords, authentication and account access. I will keep authentication information secure and will not share passwords, verification codes or access credentials with others.
    - I will protect the devices in my care from unapproved access or theft.

8. I will take care before opening links or attachments, including those apparently sent by a known contact. I will check unexpected or suspicious messages through an appropriate route and report suspected phishing or malicious content to Helen Bradley-Wyatt.

9. I will not attempt to install any personally purchased or downloaded software, including browser toolbars, or hardware without permission from the headteacher.

10. I will ensure that any personal data is kept in accordance with data protection legislation, in line with the school information security policies.
    - All personal data will be obtained and processed fairly and lawfully, only kept for specific purposes, held no longer than necessary and will be kept private and secure with appropriate security measures in place, whether used in the workplace, hosted online or accessed remotely.
    - Any data being removed from the school site, such as via email or on memory sticks or CDs, will be suitably protected. This may include data being encrypted by a method approved by the school.
    - I will only process or share personal data through school-approved systems and services and in line with the setting's data protection and information-security procedures. Any proposed new or changed use of cloud services, AI tools or other online systems involving personal data will be risk assessed and approved through the setting's agreed process before use. Where required, a Data Protection Impact Assessment will be completed.

11. I will not keep documents which contain school related sensitive or personal information, including images, files, videos, and emails, on any personal devices, such as laptops, digital cameras, and mobile phones. Where possible, I will use the school learning platform to upload any work documents and files in a password protected environment or school VPN.

12. I will not store any personal information on the school IT system, including school laptops or similar device issued to members of staff, that is unrelated to school activities, such as personal photographs, files or financial information.

13. I will ensure that school owned information systems are used lawfully and appropriately. I understand that the Computer Misuse Act 1990 makes the following criminal offences: to gain unauthorised access to computer material; to gain unauthorised access to computer material with intent to commit or facilitate commission of further offences or to modify computer material without authorisation.

14. I will not attempt to bypass any filtering and/or security systems put in place by the school

15. If I suspect a computer or system has been damaged or affected by a virus or other malware, I will report this to the headteacher as soon as possible.

16. If I have lost any school related documents or files, I will report this to Cantium and school Data Protection Officer Mrs Bradley-Wyatt as soon as possible.

17. I will follow the school image use policy when taking, using, storing or sharing images or recordings of pupil Images and recordings must always be appropriate and must only be taken using school-provided or approved equipment. I will not use personal devices, including personal mobile phones, cameras, tablets, smart watches or other wearable technology, to take images or recordings of pupils. Images and recordings will only be taken, used or shared in line with the school image use policy, safeguarding expectations, data protection requirements and consent/lawful basis arrangements.

Classroom practice

18. I understand my role and responsibilities in relation to filtering and monitoring, as explained through induction, safeguarding training and relevant school policies.

19. If I become aware of a filtering or monitoring failure, or witness or suspect accidental or deliberate access to illegal, inappropriate or harmful material, I will report this to the DSL and IT provider/staff, in line with the school child protection policy

20. I will follow school expectations for safe technology use in classrooms, remote/online learning and other working spaces, including the use of approved platforms, search tools and AI tools.

21. I will follow the setting's agreed approach to screen use. Any use of screens, devices, apps or online content will be planned, purposeful, age appropriate and supervised, and will not replace face-to-face interaction, play, physical activity, rest, care routines or real-world exploration.

22. I am aware that generative artificial intelligence (AI) tools may have many uses which could benefit our school community. However, I recognise that AI tools can also pose risks, including, but not limited to, bullying and harassment, abuse and exploitation (including child sexual abuse), privacy and data protection risks, plagiarism and cheating, and inaccurate, harmful and/or biased material. Additionally, their use can pose moral, ethical and legal concerns if not carefully managed. As such, I understand that:
    - AI tools must only be used responsibly, ethically and where the tool, purpose and use have been approved by leaders. Any new, unapproved or changed use of AI tools will be risk assessed and approved before use, in line with child protection, data protection and professional conduct expectations.
    - I understand that AI-generated content must be checked for accuracy, bias, appropriateness, copyright and safeguarding implications before it is used or shared.
    - I will not enter personal, sensitive, confidential, safeguarding, assessment or special category information, or images of pupils, staff or other identifiable individuals, into any

AI tool unless the tool has been approved for that purpose, the use has been risk assessed, consent has been obtained where required, and the leadership team has confirmed that the processing is lawful and appropriate.

- I will not add or use AI note takers, transcription tools, recording bots or automated meeting summary tools in any meeting, lesson, supervision, training or professional discussion unless this has been agreed in advance by leadership. Where approved, I will ensure that participants are made aware and their use is transparent, proportionate and in line with safeguarding, confidentiality, consent, data protection and information governance expectations.
- I will not use AI to make decisions about pupils families or staff, including decisions relating to safeguarding, behaviour, SEND, assessment, attendance, admissions, recruitment, allegations or pastoral support, without appropriate professional oversight and in line with setting policy.
- Only approved AI platforms may be used with pupils. Children must be supervised when using AI tools, and I must ensure age-appropriate use and understanding prior to use.
- I will report any concern involving AI misuse, including deepfake or manipulated content, impersonation, harmful AI-generated material, AI-facilitated bullying or harassment, or AI-generated nude/semi-nude imagery, in line with the schoolchild protection, behaviour, anti-bullying, staff conduct and data protection procedures.

23. I will promote online safety with the children in my care and will help them to develop a responsible attitude to safety online, system use and to the content they access or create by:
    - exploring online safety principles as part of an embedded and progressive curriculum and reinforcing safe behaviour whenever technology is used.
    - creating a safe environment where children feel comfortable to report concerns and say what they feel, without fear of getting into trouble or being judged for talking about something which happened to them online.
    - involving the DSL or a deputy as part of planning online safety lessons or activities to ensure support is in place for any children who may be impacted by the content.
    - informing the DSL and/or leadership team if I am teaching topics which could create unusual activity on the filtering logs, or if I believe the filtering system is placing unreasonable restrictions on teaching, learning or administration.
    - making informed decisions to ensure any online safety resources used with children are appropriate.

24. I will respect copyright and intellectual property rights and ensure my use of online platforms and tools is safe, legal and ethical; I will obtain appropriate permission to use content, and if videos, images, text, or music are protected, I will not copy, share, misuse, plagiarise, or distribute them.

Mobile phones and smart devices

25. I will ensure that my use of mobile phones and smart devices is compatible with my professional role, does not interfere with my duties, and takes place in line with the staff behaviour policy/code of conduct, mobile phone policy and the law.

26. I will model safe and professional use of mobile phones and smart devices and will support the school's expectations for pupils.

27. Where mobile phones or smart devices are used for professional purposes, such as authentication, learning activities, recording rewards or sanctions, or other agreed tasks, I will use school-provided devices where available. Where staff are permitted to use personal devices for professional purposes, this must be formally agreed by the school and managed in line with schoolpolicy.

28. Any use of a personal mobile phone or smart device for professional purposes, or in exceptional circumstances, must be transparent, necessary, proportionate and approved by the headteacher or other designated leader. Use must not compromise supervision, safeguarding, confidentiality, professional boundaries, data protection or the learning environment.

Online communication, including use of social media

29. I will ensure that my use of communication technology, including social media, is compatible with my professional role, does not interfere with my work duties, and takes place in line with the child protection policy, staff behaviour policy/code of conduct, social media policy and the law.

30. I will protect myself, my professional reputation and the reputation of the school online. I will not discuss or share data or information relating to pupils, staff, school business or parents/carers on social media.

31. My electronic communications with current and former children and parents/carers will be transparent and open to scrutiny and will only take place within clear and explicit professional boundaries.
    - I will ensure that all electronic communications take place in a professional manner via school-provided communication channels and systems, such as a school email address, user account or telephone number.
    - I will not use personal accounts, personal profiles, personal phone numbers, private messaging apps, gaming accounts or other personal communication channels to contact or communicate with children or their families, unless this has been formally approved, risk assessed and recorded by leaders.
    - I will not share any personal contact information or details with pupils such as my personal address, email address or phone number.
    - I will not share personal information about my private life with children online, through messaging, social media, gaming platforms, apps or other digital communication

channels. I will maintain appropriate professional boundaries in all digital communication.

- I will not add, follow, accept or respond to friend requests, direct messages or other personal online communication from current or former pupils or their parents/carers, where this is linked to my role, the school or could blur professional boundaries. Any attempted contact will be reported to my line manager and/or the DSL.
- Any pre-existing links, relationships or situations that affect how I apply the AUP or other relevant policies will be discussed with the DSL and/or [headteacher/manager]. This is to help safeguard pupils, staff and the wider school community by ensuring professional boundaries, safeguarding expectations and communication arrangements are clear.
- Where digital communication with children or families is required, I will follow the school's expectations about when communication should take place, including any agreed arrangements for out-of-hours contact, emergency communication or role-specific responsibilities.

Policy concerns

32. I will not upload, download, or access any materials which are illegal, such as child sexual abuse images, criminally racist material, terrorist material or adult pornography covered by the Obscene Publications Act.

33. I will not access, create, transmit, display, publish, forward, discuss, send, share or show any material or content that may be harmful, inappropriate, adult, offensive, unprofessional, or likely to harass, cause offence, inconvenience or needless anxiety to any other person. This applies when using school systems, school devices, personal devices, personal accounts, messaging apps, online platforms, social media or shared spaces. It includes content shared in staff rooms, offices, online groups or other staff communication spaces, where this takes place on school premises, during working time, or in any context linked to my role.

34. I will not engage in online or digital behaviour linked to my role that compromises safeguarding, professional boundaries, confidentiality, data protection, public confidence in my professional conduct or my ability to carry out my role.

35. I will report and record any concerns about the welfare, safety or behaviour of children or parents/carers online to the DSL in line with the school child protection policy.

36. I will report concerns about the welfare, safety, conduct, or behaviour of staff, including online, digital, device-related or technology-linked concerns, to the headteacher], in line with the school child protection policy, staff behaviour policy/code of conduct, low-level concerns procedures and/or allegations against staff policy.

Policy compliance and breaches

37. If I have any queries or questions regarding safe and professional practice online, either in school or off site, I will raise them with the DSL and/or the headteacher.

38. I understand that the school may exercise its right to monitor the use of its devices and information systems to check policy compliance and help ensure the safety of children and staff.
    - This includes monitoring all school-provided devices and school systems and networks including school-provided internet access, whether used on or offsite and may include the interception of messages and emails sent or received via school-provided devices, systems and/or networks.
    - This monitoring will be proportionate and will take place in accordance with data protection, privacy, and human rights legislation.
    - Staff will be informed about the nature, purpose and extent of monitoring through this AUP, relevant policies, privacy information and/or staff guidance.

39. I understand that if the school believes that unauthorised and/or inappropriate use of school devices, systems or networks is taking place, the school may invoke its disciplinary procedures as outlined in the staff code of conduct policy.

40. If I find myself in a situation where my online contact, device use, recording, image use or AI use could be misinterpreted, I will report this promptly to the headteacher so it can be recorded and managed transparently.

41. Any breach or concern involving online contact, device use, images, recordings, social media, AI use, confidentiality, data protection or professional boundaries must be reported to the headteacher and/or DSL without delay, even if it appears minor, accidental or unlikely to meet the harm threshold.

42. I understand that if the school believes that unprofessional or inappropriate online or technology-related activity may have compromised safeguarding, professional boundaries, confidentiality, data protection, public confidence in professional conduct or my ability to carry out my role, the concern will be considered fairly, proportionately and confidentially, in line with relevant safeguarding, staff behaviour, low-level concerns, allegations, data protection and disciplinary procedures. Where the concern may meet the harm threshold, advice will be sought and/or a referral made to the Local Authority Designated Officer (LADO) in line with local allegations procedures. Where it does not meet this threshold, it will still be recorded and responded to appropriately.

43. Where a concern involves personal data, confidential information, safeguarding information, images, recordings, AI tools, transcription tools or unauthorised sharing, the DPO/data protection lead will be informed promptly so that any data protection, information governance or reporting requirements can be considered.

44. I understand that if the school suspects criminal offences have occurred, the police will be informed where appropriate.

45. I understand that this AUP cannot cover every possible situation. If I am unsure whether any use of technology, online communication, image use, recording, personal device use, social media, AI tool or digital contact is appropriate, I will seek advice from the DSL and/or

headteacher before taking action. I will act in a way that safeguards pupils protects professional boundaries, and is open to scrutiny.

I have read, understood and agreed to comply with Hollingbourne Primary School Staff Acceptable Use of Technology Policy when using the internet and other associated technologies, both on and off site.

Name: ……

Signed: …….....

Date (DDMMYY):……..

Staff Acceptable Use of Technology Policy: Key Expectations Summary

This summary highlights key expectations from the Staff Acceptable Use of Technology Policy. It is not a replacement for the full AUP, which all staff must read, understand and follow. If there is any uncertainty, staff should refer to the full AUP and seek advice from the DSL and/or headteacher **before taking action.**

As a member of staff, I understand that I must use technology in a safe, lawful, professional and responsible way. This applies to school devices, systems, networks, accounts, online platforms, mobile phones, smart technology, artificial intelligence (AI) tools, social media and any digital communication linked to my role.

Key expectations

I will:

- use school systems, devices and accounts in line with relevant policies, including child protection, staff code of conduct, data protection, mobile phone, social media and remote/online learning policies;
- keep devices, passwords, accounts, personal data, images, recordings and confidential information secure, and report any loss, breach, concern or suspected security issue promptly;
- only use school approved systems, accounts, platforms and devices when working with or communicating with children or families, unless another approach has been formally approved, risk assessed and recorded;
- maintain clear professional boundaries in all online and digital communication, including email, messaging, social media, apps, gaming platforms and remote/online learning;
- not use personal accounts, personal profiles, private messaging apps, gaming accounts, personal phone numbers or other personal communication channels to contact children or their families, unless this has been formally approved, risk assessed and recorded by leaders;
- not share personal contact details or personal information about my private life with children online or through digital communication;
- not add, follow, accept or respond to friend requests, direct messages or personal online communication from current or former pupils or their parents/carers, where this is linked to my role, the school or could blur professional boundaries;
- discuss any pre-existing relationships or situations that may affect how I apply the AUP with the Designated Safeguarding Lead (DSL) and/or headteacher, so that safeguarding expectations, professional boundaries and communication arrangements are clear;
- follow the school's expectations about when digital communication with children and families should take place, including any agreed arrangements for out-of-hours contact, emergency communication or role-specific responsibilities;
- model safe and professional use of mobile phones and smart technology and support the school's expectations or pupils;

- use screens, devices, apps and online content with babies and young children only where purposeful, age appropriate, supervised and in line with setting policy;
- not use my own mobile phone or devices in front of children during the school day, unless this has been specifically agreed or is necessary in exceptional circumstances;
- only use artificial intelligence tools where these have been approved by leaders and are used in line with safeguarding, confidentiality, consent, data protection and information governance expectations;
- check AI-generated content for accuracy, bias, appropriateness, copyright and safeguarding implications before using or sharing it;
- not enter personal, sensitive, confidential, safeguarding, assessment or special category information, or identifiable images, into any AI tool unless the tool and purpose have been approved and the processing is confirmed as lawful and appropriate;
- report any concern involving online contact, device use, images, recordings, social media, AI use, professional boundaries, data protection or safeguarding to the DSL, headteacher Data Protection Officer (DPO) as appropriate;
- report concerns even if they appear minor or accidental;
- seek advice from the DSL and/or headteacher before taking action if I am unsure whether any use of technology, online communication, image use, recording, personal device use, social media, AI tool or digital contact is appropriate.

I understand that

- school-provided devices, systems, networks and accounts may be monitored proportionately to check policy compliance and help safeguard children and staff;
- breaches of the AUP may be considered in line with safeguarding, staff behaviour, low-level concerns, allegations, data protection and disciplinary procedures;
- where a concern may meet the harm threshold, advice will be sought and/or a referral made to the Local Authority Designated Officer (LADO), in line with local allegations procedures;
- where personal data, confidential information, images, recordings, AI tools, transcription tools or unauthorised sharing are involved, the DPO will be informed promptly;
- if criminal offences may have occurred, the police will be informed where appropriate;
- the AUP cannot cover every possible situation, so I must act in a way that safeguards pupils protects professional boundaries and is open to scrutiny.

Visitor/Volunteer Acceptable Use of Technology Policy

As a professional organisation with responsibility for safeguarding, it is important that visitors and volunteers understand our expectations for safe, lawful and responsible technology use while on site, when using school systems, or when acting in a role connected to the school This AUP helps Hollingbourne Primary School explain expectations around safeguarding, professional conduct, data protection, image use, mobile phones, online communication and reporting concerns.

Policy scope

1. I understand that this Acceptable Use of Technology Policy (AUP) applies to my use of technology systems, services, devices or information provided by the school or accessed by

me as part of my role, visit or activity with Hollingbourne Primary School. It also applies to personal devices or accounts where their use takes place on site, involves the school community, is linked to my role or visit, or could affect safeguarding, confidentiality, data protection, professional boundaries or the reputation of the school

2. I understand that this AUP should be read and followed in line with relevant school policies, including the staff behaviour policy/code of conduct, child protection policy, visitor/volunteer procedures, image use policy and mobile phone/smart device policy.

3. I am aware that this AUP does not provide an exhaustive list; visitors and volunteers should ensure that all technology use is consistent with the school ethos, school staff behaviour and safeguarding policies, national and local education and child protection guidance, and the law.

4. I will not upload, download or access any materials which are illegal, including but not limited to child sexual abuse material, criminally racist material, terrorist material or adult pornography covered by the Obscene Publications Act.

5. I will not access, create, transmit, display, publish, forward, discuss, send, share or show any material or content that may be harmful, inappropriate, adult, offensive, unprofessional, or likely to harass, cause offence, inconvenience or needless anxiety to any other person. This applies when using school systems, school devices, personal devices, personal accounts, messaging apps, online platforms, social media or shared spaces, where this takes place on school premises, during my visit/volunteering activity, or in any context linked to my role.

6. I will not engage in any online activity, digital communication or behaviour that could compromise safeguarding, professional boundaries or the reputation of the school

Data and image use

7. Where I have access to personal data, confidential information, safeguarding information, school systems, records or devices, I will only access, use or share this information where it is necessary for my agreed role, visit or activity and in line with data protection legislation and school procedures. I will not copy, download, photograph, record, forward or share information unless this has been authorised.

8. I will not take, use, store or share images or recordings of children during lessons, visits, trips, events, performances, activities or celebrations unless this has been specifically authorised by the school and is in line with the school image use policy. Where authorised, images or recordings must only be taken, used, stored or shared using school approved equipment, accounts and systems, unless leaders have made a specific, risk-assessed decision otherwise. I will not take images or recordings of pupils for personal use or share them on personal devices, personal accounts, social media, messaging apps or online groups.

Classroom practice

9. I am aware of the expectations regarding safe use of technology in the classroom and other working spaces, including appropriate supervision of pupils.

10. Where I deliver or support remote/online learning, I will comply with the school remote/online learning AUP.

11. Where I am supporting pupils. I will reinforce safe and appropriate technology use and will follow staff instructions and school policies.

12. If I witness or suspect accidental or deliberate access to illegal, inappropriate or harmful material by any member of the school community, I will report this to a Designated Safeguarding Lead (DSL) in line with the school child protection policy

13. I will respect copyright and intellectual property rights and ensure my use of online platforms and tools is safe, legal and ethical; I will obtain appropriate permission to use content, and if videos, images, text, or music are protected, I will not copy, share, misuse, plagiarise, or distribute them.

14. I will not record, transcribe, livestream, use AI note-taking tools, recording bots or automated meeting summary tools during any meeting, visit, lesson, activity or professional discussion unless this has been specifically authorised by the school and is in line with safeguarding, confidentiality, consent and data protection expectations.

Use of mobile phones and smart devices

15. In line with the school mobile phone and smart device policy, I will model safe and appropriate use of mobile phones and smart devices while on site. I will not use my own mobile phone or smart device in front of children unless this has been agreed by the school and is directly linked to my role, visit or volunteering activity. I will follow the school's expectations about where and when mobile phones and smart devices may be used or stored.

Online communication, including the use of social media

16. I will ensure that my online conduct, reputation and use of technology are compatible with my role within the school. This includes my use of email, text, social media, social networking, gaming and any other personal devices or websites.

17. Any electronic communication with pupils, parents/carers or staff as part of my role, visit or volunteering activity will take place within clear professional boundaries and be transparent and open to scrutiny.
    - Communication will take place using school approved channels, such as a school-provided email address, account, platform or telephone number.
    - I will not use personal devices, personal email, personal social media, private messaging apps, gaming accounts or personal phone numbers to contact children or their families unless this has been formally approved, risk assessed and recorded by leaders.
    - Any pre-existing relationships, links or situations that may affect how I apply this AUP will be discussed with the DSL and/or [headteacher/manager].

18. I will respect confidentiality and will not post, comment on, discuss or share information online about pupils, staff, families, incidents, activities or anything I become aware of through my role, visit or volunteering activity. This includes comments, images, videos, recordings or information shared on personal social media, messaging apps, online groups or community forums.

Policy compliance, breaches or concerns

19. If I have any queries or questions regarding safe and professional practice online either in school or off site, I will raise them with the Designated Safeguarding Lead (Mrs Allen-Harding) and/or the headteacher (Mrs Bradley-Wyatt).

20. I understand that the school may exercise its right to monitor the use of its devices and information systems to check policy compliance and help ensure the safety of children and staff.
    - This includes monitoring all school-provided devices and school systems and networks, including school-provided internet access, whether used on or offsite, and may include the interception of messages and emails sent or received via school-provided devices, systems and/or networks.
    - This monitoring will be proportionate and will take place in accordance with data protection, privacy and human rights legislation.

21. I will report and record any concerns about the welfare, safety or behaviour of children or parents/carers online to the DSL, in line with the school child protection policy.

22. I will report concerns about the welfare, safety, conduct or behaviour of staff, including online, digital, device-related, image-related or technology-linked concerns, to the headteacher, in line with the school child protection policy, staff behaviour/code of conduct, low-level concerns procedures and/or allegations against staff policy.

23. I understand that if the school believes that illegal, unauthorised or inappropriate use, unacceptable behaviour, or a breach of this AUP has taken place, action may be taken in line with relevant safeguarding, behaviour, complaints, volunteer, contractor, visitor, data

protection, low-level concerns or allegations procedures, as appropriate. This may include ending or restricting access to the site, systems or activities, informing an employer/agency/organisation, seeking advice from the LADO, informing the DPO/data protection lead, or contacting the police where appropriate.

24. Any breach or concern involving online contact, device use, images, recordings, social media, AI use, confidentiality, data protection or professional boundaries must be reported to the DSL and/or headteacher without delay, even if it appears minor, accidental or unlikely to meet the harm threshold.

25. Where a concern involves personal data, confidential information, safeguarding information, images, recordings, AI tools, transcription tools or unauthorised sharing, the Data Protection Officer (DPO) will be informed promptly so that any data protection, information governance or reporting requirements can be considered.

26. I understand that this AUP cannot cover every possible situation. If I am unsure whether any use of technology, online communication, image use, recording, personal device use, social media, AI tool or digital contact is appropriate, I will seek advice from the DSL and/or headteacher.

I have read, understood and agreed to comply with Hollingbourne Primary School visitor/volunteer Acceptable Use of Technology Policy when using the internet and other associated technologies, both on and off site.

Name of visitor/volunteer: ……..……

Signed: ……..

Date (DDMMYY)…….....

Wi-Fi Acceptable Use Policy

As a professional organisation with responsibility for safeguarding children, all users must understand the boundaries and expectations when using the school Wi-Fi. Users are expected to use Wi-Fi safely, lawfully and responsibly, and to take reasonable steps to protect devices, data and information systems from infection, unauthorised access, damage, loss, abuse and theft.

This is not an exhaustive list. All users are reminded that technology use should be consistent with the school ethos, relevant policies and the law.

1. The school provides Wi-Fi for education purposes only.

2. Use of the Wi-Fi falls under Hollingbourne Primary School Acceptable Use of Technology Policy (AUP), the child protection policy, behaviour policy/code of conduct, data protection/security policies and any other relevant policies. All pupils, staff, visitors and volunteers using the Wi-Fi must comply with these expectations.

3. The school reserves the right to limit, restrict, withdraw or manage Wi-Fi access where necessary to maintain safeguarding, security, network reliability or fair use of network resources.

4. School owned information systems, including Wi-Fi, must be used lawfully. I understand that the Computer Misuse Act 1990 makes it a criminal offence to gain unauthorised access to computer material, gain unauthorised access with intent to commit or facilitate further offences, or modify computer material without authorisation.

5. I will take reasonable steps to ensure that any personal device connected to school Wi-Fi is appropriately secure, for example by using security updates, antivirus protection where appropriate, and secure passwords/PINs.
6. I will respect system security and will not share passwords, Wi-Fi access details or security information. I will not attempt to bypass school security, filtering or monitoring systems, or download unauthorised software, applications or files.

7. I will not use school Wi-Fi to access, create or share illegal or harmful content, compromise another person’s safety or privacy, interfere with systems, or breach relevant school policies.

8. I will not use school Wi-Fi to access, store, send or share confidential, personal or safeguarding information unless this has been specifically authorised and is in line with school data protection and safeguarding procedures.

9. Staff using school Wi-Fi on personal devices remain subject to the staff behaviour policy/code of conduct, Staff AUP, mobile phone/smart device policy, data protection expectations, and relevant safeguarding and disciplinary procedures.

10. The school takes reasonable and proportionate steps to manage the security of its Wi-Fi service. However, no wireless or internet service can be guaranteed to be free from all risk.

Where personal devices are permitted to connect to the school Wi-Fi, users do so at their own discretion and are expected to keep their devices secure. Any concerns about Wi-Fi security, filtering, monitoring or device safety should be reported to the DSL or identified technical contact.

11. I will report any online safety concerns, filtering breaches, security concerns, or access to inappropriate materials to the Designated Safeguarding Lead (Mrs Allen-Harding) or identified technical contact as soon as possible. If I have any queries about safe behaviour online, I will speak to the DSL, identified technical contact or headteacher (Mrs Bradley-Wyatt).

12. I understand that activity carried out through school Wi-Fi may be monitored and recorded to check policy compliance, protect systems and help keep users safe, including where the Wi-Fi is accessed using a personal device. This does not mean that the school can monitor other activity or information held on the personal device. Monitoring will be proportionate and will take place in accordance with data protection, privacy and human rights legislation.

13. If the school suspects that unauthorised or inappropriate use, unacceptable behaviour, a data protection concern, a safeguarding concern or criminal activity may have taken place, access may be restricted or withdrawn and the concern may be managed in line with relevant school procedures. Where appropriate, this may include informing the DSL, Data Protection Officer, headteacher/manager, employer/organisation, LADO or police.

I have read, understood and agreed to comply with Hollingbourne Primary School Wi-Fi Acceptable Use Policy.

Name ……**Signed** ……....**Date (DDMMYY)**…….

Template Acceptable Use Policy (AUP) for Remote/Online Learning

Additional information and guides on specific platforms can be found at:

- LGfL: Safeguarding Considerations for Remote Learning
- SWGfL: Which Video Conference platform is best?

Further information and guidance for SLT and DSLs regarding remote learning:

- SWGfL: Safer Remote Learning
- NSPCC: Undertaking remote teaching safely
- Safer Recruitment Consortium: Guidance for safer working practice

Remote/Online Learning AUP Template - Staff Statements

Hollingbourne Primary School Staff Remote/Online Learning AUP

The Remote/Online Learning Acceptable Use Policy (AUP) is in place to safeguard all members of Hollingbourne Primary School community when taking part in remote/online learning, for example following any full or partial school closures.

Leadership oversight and approval

1. Remote/online learning will only take place using Teams.
    - Teams has been assessed and approved by the headteacher.

2. Staff will only use school approved professional accounts with children and/or parents/carers.
    - Use of any personal accounts to communicate with children and/or parents/carers is not permitted.
        - Any pre-existing relationships or situations which mean this cannot be complied with will be discussed with Mrs Allen-Harding, Designated Safeguarding Lead (DSL).
    - Staff will use work provided equipment where possible**.**

3. Online contact with children, parents/carers will not take place outside of the operating times as defined by SLT:
    - Between 8.45am and 3.10pm.

4. All remote/online lessons will be formally timetabled**;** a member of SLT is able to drop in at any time.

5. Live-streamed remote/online learning sessions will only be held with approval and agreement from the headteacher.

Data Protection and Security

6. Any personal data used by staff and captured by Teams when delivering remote learning will be processed and stored with appropriate consent and in accordance with our data protection policy.

7. All remote/online learning and any other online communication will take place in line with current school confidentiality expectations as outlined in our Data Protection policy.

8. Participants will be informed about any activity that Teams records or retains, such as chat messages, attendance, shared files or audio/video recording and how this information will be used.

9. Staff will not record lessons or meetings using personal equipment unless agreed and risk assessed by SLT and in line with our data protection policy requirements.

10. Only members of the Hollingbourne Primary School community will be given access to Teams.

11. Access to Teams will be managed in line with current IT security expectations.

12. AI note takers, transcription tools, recording bots or automated meeting summaries must not be used in remote/online learning, meetings or training unless this has been approved in advance by leaders and is managed in line with safeguarding, consent, confidentiality and data protection requirements.

Session management

13. Staff will record the length, time, date, and attendance of any sessions held.

14. Appropriate privacy and safety settings will be used to manage access and interactions. This includes:

15. Live sessions will follow the school's agreed staffing, oversight and audit arrangements.

16. Live 1:1 sessions will only take place with approval from the headteacher.

17. A pre-agreed invitation detailing the session expectations will be sent to those invited to attend.
    - Access links should not be made public or shared by participants.
    - Children and/or parents/carers should not forward or share access links.
    - If children or parents/carers believe a link should be shared with others, they will discuss this with the member of staff running the session first.
    - Staff will explain any expectations about the location from which children take part. These will reflect their age, needs, privacy, home circumstances and the nature of the session.

18. Alternative approaches and/or access will be provided to those who do not have access.

Behaviour expectations

19. Staff will model safe practice and moderate behaviour online during remote sessions as they would in the classroom.

20. All participants are expected to behave in line with existing school policies and expectations. This includes:
    - Appropriate language will be used by all attendees.
    - Staff will not take or record images for their own personal use.

- Setting decisions about if other attendees can or cannot record events for their own use, and if so, any expectations or restrictions about onward sharing.

21. Staff will remind attendees of behaviour expectations and reporting mechanisms at the start of the session.

22. When sharing videos and/or live streaming, participants are required to:
    - wear appropriate dress.
    - ensure backgrounds of videos are neutral (blurred if possible).
    - ensure that personal information and/or unsuitable personal items are not visible, either on screen or in video backgrounds.

23. Educational resources will be used or shared in line with our existing teaching and learning policies, taking licensing and copyright into account.

Policy Breaches and Reporting Concerns

24. Participants are encouraged to report concerns during remote and/or live-streamed sessions.

25. If inappropriate language or behaviour takes place, participants involved will be removed by staff, the session may be terminated, and concerns will be reported to the headteacher (Mrs Bradley-Wyatt).

26. Inappropriate online behaviour will be responded to in line with existing policies such as acceptable use of technology, allegations against staff, anti-bullying and behaviour.

27. Sanctions for deliberate misuse may include: restricting or removing use, seeking police or other appropriate advice where behaviour may present risks to safety.

28. Any safeguarding concerns will be reported to Mrs Allen-Harding, Designated Safeguarding Lead, in line with our child protection policy.

I have read and understood the Hollingbourne Primary School Acceptable Use Policy (AUP) for remote/online learning.

Staff Member Name: ……

29.

Date…….

Remote/Online Learning AUP Template – Pupil/Student Statements

Hollingbourne Primary School Pupil Remote/Online Learning AUP

1. I understand that:
    - these expectations are in place to help keep me safe when I am learning at home using Microsoft Teams.
    - I should read and talk about these rules with my parents/carers.
    - remote/online learning will only take place using Teams and during usual school times.
        - my use of Teams is monitored to help keep me safe.

2. Only members of the Hollingbourne Primary School community can access Teams.
    - I will only use my school provided email accounts and login to access remote learning.
    - I will use privacy settings as agreed with my school setting.
    - I will not share my login/password with others.
    - I will not share any access links to remote learning sessions with others.

3. When taking part in remote/online learning I will behave as I would in the classroom. This includes:
    - Using appropriate language;
    - Being respectful to others;
    - Not interrupting others;
    - Not recording images or content without agreement from the teacher;
    - Listening carefully to all instructions.

4. When taking part in live sessions I will:
    - mute my video and microphone.
    - wear appropriate clothing and be in a suitable location.
    - ensure backgrounds of videos are neutral and personal information/content is not visible.
    - use appropriate alternative backgrounds.
    - attend the session in full. If for any reason I cannot attend a session in full, I will let my teacher know.
    - I will take part from a suitable location, following any arrangements agreed with the school. I will take reasonable steps to protect my privacy and the privacy of other people in my home.

5. If I am concerned about anything that takes place during remote/online learning, I will:
    - Report my concerns to my teacher;
    - Tell my parents/carers.

6. I understand that inappropriate online behaviour or concerns about my or others safety during remote/online learning will be taken seriously. This could include:
    - Restricting or removing access to learning;
    - Informing parents/carers of concerns;
    - Following safeguarding procedures;
    - Seeking advice from specialists (where appropriate).

I have read and understood the Hollingbourne Primary School Pupil Acceptable Use Policy (AUP) for remote learning.

Name……. Signed……..…….

Class……..…… Date…….…….

Parent/Carer's Name……..…….....

Parent/Carer's Signature…….…….

Date…….…….