



# Internet Acceptable Use Policy

Policy Creation & Review	
Author(s)	Gemma Hitch
Last review date	01.09.22
Ratified by Governing body and headteacher	28.9.22
Previous Review Date(s)	01.09.21
Next Review Date	September 2023

**This policy will be reviewed at least annually and or following any updates to national and local guidance and procedures.**

## **Key Contact Personnel in School**

Designated Safeguarding Lead: Mrs Gemma Hitch

Deputy Designated Safeguarding Lead: Mrs Lorna Lloyd

Named Safeguarding Governor: Mr Nick Hillman

# Contents

## **Children/Pupils/Student Acceptable Use of Technology Sample Statements**

Early Years and Key Stage 1 (0-6)

Key Stage 2 (7-11)

Pupils with SEND

Children/Pupils/Student Acceptable Use Policy Agreement Form

## **Acceptable Use of Technology Sample Statements/Forms for Parents/Carers**

Parent/Carer Acknowledgement Form

Sample Parent/Carer Acceptable Use of Technology Policy

## **Acceptable Use of Technology for Staff, Visitors and Volunteers**

Staff Acceptable Use of Technology Policy

Visitor and Volunteer Acceptable Use of Technology Policy

Wi-Fi Acceptable Use Policy

## **Remote/Online Learning AUPs**

Guidance Notes

Staff Sample Statements

Pupil/Student Sample Statements

# Pupil Acceptable Use of Technology Statements

## Early Years

- 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 1

I understand that the [school](#) Acceptable Use Policy will help keep me safe and happy online.

- I only use the internet when an adult is with me.
- I only click on online links and buttons when I know what they do. If I am not sure, I ask an adult first.
- I keep my personal information and passwords safe.
- I only send messages online which are polite and friendly.
- I know the [school](#) can see what I am doing online when I use [school](#) computers and tablets, including when I am at home.
- I always tell an [adult/teacher/member of staff](#) if something online makes me feel upset, unhappy, or worried.
- I can visit [www.thinkuknow.co.uk](http://www.thinkuknow.co.uk) to learn more about keeping safe online.
- I know that if I do not follow the rules:
  - **My parents will be informed**
  - **I may be unable to use the internet for a period of time**
- I have read and talked about these rules with my parents/carers.

## 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 behave online the same way as I behave in the classroom.
- I only send messages which are polite and friendly.
- I will only post pictures or videos on the internet if they are safe and appropriate, and if I have permission.
- I only talk with, and open messages, from people I know.
- I will only click on links if I know they are safe.
- I know that people I meet online may not always be who they say they are. If someone online suggests meeting up, I will immediately talk to an adult.

### Learning

- I am not permitted to use my own personal smart devices and/or mobile phone at **school**.
- I always ask permission from an adult before using the internet.
- I only use websites and search engines that **my teacher** has chosen.
- I use **school** devices for **school** work unless I have permission otherwise.
- If I need to learn online at home, I will follow the **school remote/online** learning AUP.

### Trust

- I know that not everything or everyone online is honest or truthful.
- I will check content on various sources like other websites, books or with a trusted adult.
- I always credit the person or source that created any work, images, or text I use.

### 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.

### 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** devices and systems are monitored to help keep me safe, including when I use them at home.
- I have read and talked about these rules with my parents/carers.
- I can visit [www.thinkuknow.co.uk](http://www.thinkuknow.co.uk) and [www.childline.org.uk](http://www.childline.org.uk) to learn more about being safe online.
- I know that if I do not follow the **school** rules then:
  - **My parents will be informed**
  - **I may be unable to use the internet for a period of time**

## Tell

- If I see anything online that I should not or that makes me feel worried or upset, I will minimise the page and tell an adult straight away. **Amend to reflect your approach e.g. shut the laptop lid, turn off the screen.**
- If I am aware of anyone being unsafe with technology, I will report it to [a teacher](#).
- I know it is not my fault if I see, or someone sends me, something bad online. I always talk to an adult if I am not sure about something or if something happens online that makes me feel worried or frightened.

# Pupils with Special Educational Needs and Disabilities (SEND)

## Learners with SEND functioning at Levels P4 –P7

- I ask a grown-up if I want to use the computer.
- I make good choices on the computer.
- I use kind words on the internet.
- If I see anything that I do not like online, I tell a grown up.
- I know that if I do not follow the **school** rules then:
  - **My parents will be informed**
  - **I may be unable to use the internet for a period of time**

## 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 the computer.
- I do not tell strangers my name on the internet.
- I know that if I do not follow the **school** rules then:
  - **My parents will be informed**
  - **I may be unable to use the internet for a period of time**

### 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 that I do not like online, 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 keep my information private on the internet.
- I am careful if I share photos online.
- I know that if I do not follow the **school** rules then:
  - **My parents will be informed**
  - **I may be unable to use the internet for a period of time**

**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 I do not like, I will tell [a teacher](#).

# Parent/Carer AUP Acknowledgement

## Laddingford St Mary's Primary School Pupil Acceptable Use of Technology Policy Acknowledgment

1. I have read and discussed Laddingford St Mary's Primary School pupil acceptable use of technology policy (AUP) with my child and understand that the AUP will help keep my child safe online.
2. I understand that the AUP applies to my child's use of school devices and systems on site and at home and personal use where there are safeguarding and/or behaviour concerns. This may include if online behaviour poses a threat or causes harm to another pupil, could have repercussions for the orderly running of the school, if a pupil is identifiable as a member of the school, or if the behaviour could adversely affect the reputation of the school.
3. I am aware that any use of school devices and systems are appropriately filtered and may be monitored for safety and security reason to keep my child safe and to ensure policy compliance. This monitoring will be proportionate and will take place in accordance with data protection, privacy, and human rights legislation.
4. I am aware that the school mobile and smart technology policy states that my child cannot use personal device and mobile and smart technology on site. **Mobile phones should be handed to the office, kept switched off during lessons/on site.**
5. I understand that my child needs a safe and appropriate place to access remote/online learning, for example, if the school is closed in response to Covid-19. I will ensure my child's access to remote/online learning is appropriately supervised and any use is in accordance with the school remote learning AUP. .
6. I understand that the school will take every reasonable precaution, including implementing appropriate monitoring and filtering systems, to ensure my child is safe when they use school devices and systems. I understand that the school cannot ultimately be held responsible for the nature and content of materials accessed online or if my child is using personal mobile or smart technologies.
7. I and my child are aware of the importance of safe online behaviour and will not deliberately upload or share any content that could upset, threaten the safety of or offend any member of the school community, or content that could adversely affect the reputation of the school.
8. I understand that the school will contact me if they have concerns about any possible breaches of the AUP or have any concerns about my child's safety online.

9. I will inform the [school](#) (for example speaking to my child's teacher and/or the Designated Safeguarding Lead) or other relevant organisations if I have concerns over my child's or other members of the [school](#) community's safety online.
10. I know that my child will receive online safety education to help them understand the importance of safe use of technology and the internet, both in and out of [school](#).
11. I understand my role and responsibility in supporting the [schools](#) online safety approaches and safeguarding my child online. I will use parental controls, supervise access and will encourage my child to adopt safe use of the internet and other technology at home, as appropriate to their age and understanding.



# Pupil/Student Acceptable Use Policy Agreement and Parent Acknowledgement Form

## Laddingford St Mary's 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 use my own equipment out of the school, including communicating with other members of the school or when accessing school systems.

Name..... Signed.....

Class..... Date.....

Parent/Carer's Name..... (If appropriate)

Parent/Carer's Signature..... (If appropriate)

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 members of staff are expected to use Laddingford St Mary's Primary School IT systems in a professional, lawful, and ethical manner. To ensure that members of staff understand their professional responsibilities when using technology and provide appropriate curriculum opportunities for [pupils](#), they are asked to read and sign the staff Acceptable Use of Technology Policy (AUP).

Our AUP is not intended to unduly limit the ways in which members of staff teach or use technology professionally, or indeed how they use the internet personally, however the AUP will help ensure that all staff understand Laddingford St Mary's Primary School expectations regarding safe and responsible technology use and can manage the potential risks posed. The AUP will also help to ensure that [school](#) systems are protected from any accidental or deliberate misuse which could put the safety and security of our systems or members of the community at risk.

### Policy scope

1. I understand that this AUP applies to my use of technology systems and services provided to me or accessed as part of my role within Laddingford St Mary's Primary School both professionally and personally. This may include use of laptops, mobile phones, tablets, digital cameras, and email as well as IT networks, data and data storage, remote learning and online and offline communication technologies.
2. I understand that Laddingford St Mary's Primary School Acceptable Use of Technology Policy (AUP) should be read and followed in line with the [school \*\*child protection\*\* policy](#), staff [code of conduct](#).
3. I am aware that this AUP does not provide an exhaustive list; 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 only use the equipment and internet services provided to me by the **school** for example **school** provided laptops, tablets, mobile phones, and internet access, when working with **pupils**. **If I wish to use a personal device I will seek permission from the Headteacher before doing so.**
5. I understand that any equipment and internet services provided by my workplace is intended for education purposes and/or professional use and should only be accessed by members of staff. Reasonable personal use of setting IT systems and/or devices by staff **is** allowed.

## Data and system security

6. 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 use a 'strong' password to access **school** systems. **A strong password has numbers, letters and symbols, with 8 or more characters, does not contain a dictionary word and is only used on one system.**
  - I will protect the devices in my care from unapproved access or theft. **For example by not leaving devices visible or unsupervised in public places.**
7. I will respect **school** system security and will not disclose my password or security information to others.
8. I will not open any hyperlinks or attachments in emails unless they are from a known and trusted source. If I have any concerns about email content sent to me, I will report them to the **IT system manager**.
9. I will not attempt to install any personally purchased or downloaded software, including browser toolbars, or hardware without permission from the **IT system manager**.
10. I will ensure that any personal data is kept in accordance with the Data Protection legislation, including GDPR 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**.
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.

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 [ICT Support Provider/Team/lead \(Perry Everard via the school office\)](#) as soon as possible.
16. If I have lost any [school](#) related documents or files, I will report this to the [ICT Support Provider/Team/lead \(Perry Everard via the school Office\)](#) and [school](#) Data Protection Officer ([Colin Howard](#)) as soon as possible.
17. Any images or videos of [pupils](#) will only be used as stated in the [school](#) camera and image use policy. I understand images of [pupils](#) must always be appropriate and should only be taken with [school](#) provided equipment and only be taken/published where [pupils](#) and/or parent/carers have given explicit written consent.

## **Classroom practice**

18. I am aware of the expectations relating to safe technology use in the classroom, safe remote learning, and other working spaces as listed in [child protection including online safety, remote learning AUP](#).
19. I have read and understood the [school](#) mobile and smart technology and social media policies.
20. I will promote online safety with the [pupils](#) 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 [pupils](#) feel comfortable to report concerns and say what they feel, without fear of getting into trouble and/or be judged for talking about something which happened to them online.
  - involving the Designated Safeguarding Lead (DSL) ([name](#)) or a deputy ([names](#)) as part of planning online safety lessons or activities to ensure support is in place for any [pupils](#) who may be impacted by the content.

- make informed decisions to ensure any online safety resources used with **pupils** is appropriate.

21. I will report any filtering breaches (such as access to illegal, inappropriate, or harmful material) to the DSL in line with the [school child protection/online safety policy](#).

22. I will respect copyright and intellectual property rights; I will obtain appropriate permission to use content, and if videos, images, text, or music are protected, I will not copy, share, or distribute or use them.

## **Mobile devices and smart technology**

23. I will ensure that my use of mobile devices and smart technology is compatible with my professional role, does not interfere with my work duties and takes place in line with the [staff behaviour policy/code of conduct](#) and the [school](#) mobile technology policy and the law.

## **Online communication, including use of social media**

24. I will ensure that my use of communication technology, including use of social media is compatible with my professional role, does not interfere with my work duties and takes place in line with the [child protection/online safety policy](#), [staff code of conduct](#), social media policy and the law.

25. As outlined in the staff [behaviour policy/code of conduct](#) and [school](#) social media policy:

- I will take appropriate steps to protect myself and my reputation, and the reputation of the [school](#), online when using communication technology, including the use of social media.
- I will not discuss or share data or information relating to [pupils](#), staff, [school](#) business or parents/carers on social media.

**Leaders should ensure there is a policy in place which addresses expectations regarding staff use of social media; a template social media policy can be found [here](#). If this is not addressed in a separate policy, additional details and expectations should be incorporated in this AUP.**

26. My electronic communications with current and past [pupils](#) 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](#) approved and/or provided communication channels and systems, such as a [school](#) email address, user account or telephone number.
- I will not share any personal contact information or details with [pupils](#), such as my personal email address or phone number.
- I will not add or accept friend requests or communications on personal social media with current or past [pupils](#) and/or their parents/carers.

- If I am approached online by a current or past **pupils** or parents/carers, I will not respond and will report the communication to my line manager and (**name**) Designated Safeguarding Lead (DSL).
- Any pre-existing relationships or situations that compromise my ability to comply with the AUP **or other relevant policies** will be discussed with the headteacher

## Policy concerns

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

28. I will not attempt to access, create, transmit, display, publish or forward any material or content online that **may be harmful**, inappropriate or likely to harass, cause offence, inconvenience, or needless anxiety to any other person.

29. I will not engage in any online activities or behaviour that could compromise my professional responsibilities or bring the reputation of the **school** into disrepute.

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

**31. I will report concerns about the welfare, safety, or behaviour of staff online to the headteacher, in line with school child protection policy and/or the allegations against staff policy.**

## Policy Compliance and Breaches

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

33. I understand that the **school** may exercise its right to monitor the use of its information systems, including internet access and the interception of **messages/emails on our systems**, to monitor policy compliance and to ensure the safety of **pupils** and staff. This monitoring will be proportionate and will take place in accordance with data protection, privacy, and human rights legislation.

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

35. I understand that if the **school** believe that unprofessional or inappropriate online activity, including behaviour which could bring the **school** into disrepute, is taking place online, the **school** may invoke its disciplinary procedures as outlined in the **staff behaviour policy/code of conduct**.

36. I understand that if the [school](#) suspects criminal offences have occurred, the police will be informed.

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

Name of staff member: .....

Signed: .....

Date (DDMMYY).....

## Visitor and Volunteer Acceptable Use of Technology Policy

As a professional organisation with responsibility for safeguarding, it is important that all members of the community, including visitors and volunteers, are aware of our behaviour expectations and their professional responsibilities when using technology.

This AUP will help Laddingford St Mary's Primary School ensure that all visitors and volunteers understand the [schools](#) expectations regarding safe and responsible technology use.

### Policy scope

1. I understand that this Acceptable Use of Technology Policy (AUP) applies to my use of technology systems and services provided to me or accessed as part of my role within Laddingford St Mary's Primary School, both professionally and personally. This may include use of laptops, mobile phones, tablets, digital cameras, and email as well as IT networks, data and data storage, remote learning systems and communication technologies.
2. I understand that Laddingford St Mary's Primary School AUP should be read and followed in line with the [school staff behaviour policy/code of conduct](#).
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.

### Data and image use

4. I understand that I [am not](#) allowed to take images or videos of [pupils](#) [without express permission from a member of staff](#). Any images or videos of [pupils](#) will only be taken in line with the [school](#) camera and image use policy ([link](#)). **Remove if visitors/volunteers are not allowed to take mages/videos.**

### Classroom practice

5. I am aware of the expectations regarding safe use of technology in the classroom and other working spaces, including appropriate supervision of [pupils](#).
6. I will support staff in reinforcing safe behaviour whenever technology is used on site and I will promote online safety with the [pupils](#) in my care.
7. I will immediately report any filtering breaches (such as access to illegal, inappropriate, or harmful material) to the Designated Safeguarding Lead (DSL) ([Gemma Hitch](#)) in line with the [school child protection/online safety](#) policy.

8. I will respect copyright and intellectual property rights; I will obtain appropriate permission to use content, and if videos, images, text, or music is protected, I will not copy, share, or distribute or use it..

### **Use of mobile devices and smart technology**

9. In line with the [school mobile and smart](#) technology policy, I understand that mobile and smart devices are only permitted to be used in the staffroom.

### **Online communication, including the use of social media**

10. I will ensure that my online reputation and use of technology and is 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.
- I will take appropriate steps to protect myself online as outlined in the [child protection/online safety/social media policy](#).
  - I will not discuss or share data or information relating to [pupils](#), staff, [school](#) business or parents/carers on social media.
  - I will ensure that my use of technology and the internet will not undermine my role, interfere with my duties and will be in accordance with the [school code of conduct/behaviour policy](#) and the law.
11. My electronic communications with [pupils](#), parents/carers and other professionals will only take place within clear and explicit professional boundaries and will be transparent and open to scrutiny.
- All communication will take place via [school](#) approved communication channels such as via a [school](#) provided email address, account or telephone number.
  - Communication will not take place via personal devices or communication channels such as via my personal email, social networking account or mobile phone number.
  - Any pre-existing relationships or situations that may compromise [my ability to comply with](#) this will be discussed with the headteacher

### **Policy compliance, breaches or concerns**

12. 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 headteacher
13. I will not upload, download, or access any materials which are illegal, such as child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act.
14. I will not attempt to access, create, transmit, display, publish or forward any material or content online that is inappropriate or likely to harass, cause offence, inconvenience, or needless anxiety to any other person.

15. I will not engage in any online activities or behaviour that could compromise my professional responsibilities or bring the reputation of the school into disrepute.
16. I understand that the school may exercise its right to monitor the use of school information systems, including internet access and the interception of emails/messages on school systems, to monitor policy compliance and to ensure the safety of pupils, staff and visitors/volunteers. This monitoring will be proportionate and will take place in accordance with data protection, privacy, and human rights legislation.
17. I will report and record concerns about the welfare, safety or behaviour of pupils or parents/carers online to the Designated Safeguarding Lead (Gemma Hitch) in line with the school child protection policy.
18. I will report concerns about the welfare, safety, or behaviour of staff online to the headteacher/manager, in line with the allegations against staff policy.
19. I understand that if the school believes that unauthorised and/or inappropriate use, or unacceptable or inappropriate behaviour is taking place online, the school may invoke its disciplinary procedures.
20. I understand that if the school suspects criminal offences have occurred, the police will be informed.

**I have read, understood and agreed to comply with Laddingford St Mary's 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 children's safeguarding it is important that all members of the school community are fully aware of the school boundaries and requirements when using the school Wi-Fi systems and take all possible and necessary measures to protect data and information systems from infection, unauthorised access, damage, loss, abuse and theft.

This is not an exhaustive list, and all members of the school community are reminded that technology use should be consistent with our ethos, other appropriate policies, and the law.

1. The school provides Wi-Fi for the school community and allows access for educational use only
2. I am aware that the school will not be liable for any damages or claims of any kind arising from the use of the wireless service. The school takes no responsibility for the security, safety, theft, insurance, and ownership of any device used within the school premises that is not the property of the school.
3. The use of technology falls under Laddingford St Mary's Primary School Acceptable Use of Technology Policy (AUP), online safety policy and behaviour policy which all pupils /staff/visitors and volunteers must agree to and comply with.
4. The school reserves the right to limit the bandwidth of the wireless service, as necessary, to ensure network reliability and fair sharing of network resources for all users.
5. School owned information systems, including Wi-Fi, must be used lawfully; 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.
6. I will take all practical steps necessary to make sure that any equipment connected to the school service is adequately secure, such as up-to-date anti-virus software, systems updates.
7. The school wireless service is not secure, and the school cannot guarantee the safety of traffic across it. Use of the school wireless service is done at my own risk. By using this service, I acknowledge that security errors and hacking are an inherent risk associated with any wireless network. I confirm that I knowingly assume such risk.
8. The school accepts no responsibility for any software downloaded and/or installed, email opened, or sites accessed via the school wireless service's connection to the internet. Any damage done to equipment for any reason including, but not limited to, viruses, identity theft, spyware, plug-ins or other internet-borne programs is my sole responsibility; and I indemnify and hold harmless the school from any such damage.

9. I will respect system security; I will not disclose any password or security information that is given to me. To prevent unauthorised access, I will not leave any information system unattended without first logging out or locking my login as appropriate.
10. I will not attempt to bypass any of the [school](#) security and filtering systems or download any unauthorised software or applications.
11. My use of [school](#) Wi-Fi will be safe and responsible and will always be in accordance with the [school](#) AUP and the law including copyright and intellectual property rights. This includes the use of email, text, social media, social networking, gaming, web publications and any other devices or websites.
12. I will not upload, download, access or forward any material which is illegal or inappropriate or may cause harm, distress or offence to any other person, or anything which could bring the [school](#) into disrepute.
13. I will report any online safety concerns, filtering breaches or receipt of inappropriate materials to the Designated Safeguarding Lead ([Gemma Hitch](#)) as soon as possible.
14. If I have any queries or questions regarding safe behaviour online, I will discuss them with Headteacher
15. I understand that my use of the [school](#) Wi-Fi may be monitored and recorded to ensure policy compliance in accordance with privacy and data protection legislation. If the [school](#) suspects that unauthorised and/or inappropriate use or unacceptable or inappropriate behaviour may be taking place, then the [school](#) may terminate or restrict usage. If the [school](#) suspects that the system may be being used for criminal purposes, the matter will be brought to the attention of the relevant law enforcement organisation.

**I have read, understood and agreed to comply with Laddingford St Mary's Primary School Wi-Fi Acceptable Use Policy.**

Name .....

Signed: .....Date (DDMMYY).....

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

## Remote/Online Learning AUP Template - Staff Statements

### Laddingford St Mary's Primary School Staff Remote/Online Learning AUP

The Remote/Online Learning Acceptable Use Policy (AUP) is in place to safeguarding all members of school name 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 Google Classroom
  - Google Classroom has been assessed and approved by the Headteacher.
2. Staff will only use school managed or specific, approved professional accounts with pupils and/or parents/carers
  - Use of any personal accounts to communicate with pupils and/or parents/carers is not permitted.
    - Any pre-existing relationships or situations which mean this cannot be complied with will be discussed with Gemma Hitch, Designated Safeguarding Lead (DSL).
  - Staff will use work provided equipment where possible e.g. a school laptop, tablet, or other mobile device.
3. Online contact with pupils and/or parents/carers will not take place outside of the operating times as defined by SLT:
  - 8am to 5pm
4. All remote/online lessons will be formally timetabled; a member of SLT, DSL and/or the Headteacher 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 Google Classroom 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.
8. 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.

9. Only members of the Laddingford St Mary's Primary School community will be given access to **Google Classroom**

### **Session management**

10. Staff will record the length, time, date, and attendance of any sessions held.
11. Appropriate privacy and safety settings will be used to manage access and interactions. This includes:
- **disabling/limiting chat, staff not permitting children/young people to share screens, keeping meeting IDs private, use of waiting rooms/lobbies or equivalent.**
12. When live streaming with **pupils**:
- contact will be made via **children's/pupils/students school** provided email accounts **and/or** logins..
  - staff will **mute/disable children's/pupils/students'** videos and microphones.
13. 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.
  - **Pupils and/or** parents/carers should not forward or share access links.
  - If **pupils** or parents/carers believe a link should be shared with others, they will discuss this with the member of staff running the session first.
  - **Pupils** are encouraged to attend lessons in a shared/communal space or room with an open door and/or when appropriately supervised by a parent/carer or another appropriate adult.
14. Alternative approaches **and/or** access will be provided to those who do not have access.

### **Behaviour expectations**

15. Staff will model safe practice and moderate behaviour online during remote sessions as they would in the classroom.
16. 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.**

17. Staff will remind attendees of behaviour expectations and reporting mechanisms at the start of the session.
18. 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.**
19. 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**

20. Participants are encouraged to report concerns during remote **and/or** live-streamed sessions.
21. 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 **name and role**.
22. 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.
23. Sanctions for deliberate misuse may include **Insert details e.g. restricting/removing use, contacting police if a criminal offence has been committed.**
24. Any safeguarding concerns will be reported to **name**, Designated Safeguarding Lead, in line with our child protection policy.

**I have read and understood the **Laddingford St Mary's Primary School Acceptable Use Policy (AUP)** for remote/online learning.**

Staff Member Name: .....

Date.....