Acceptable Use Policies

Including staff AUP, learner AUP and remote learning AUP

Acceptable Use Policies (AUPs) for Children, Young People, Parents/Carers, Staff, Volunteers, Visitors and other School Community Members

Approved by Governing Body

Adapted with kind permission of Kent County Council Online safety (e-Safety) Strategy Group

Early Years & Key Stage 1 Pupils (0-7)

Acceptable Use Policy:

Early Years and KS1 (0-7)

I understand that Whinfield Primary 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 links and buttons when I know what they do
- I keep my personal information and passwords safe online
- I only send messages online which are polite and friendly
- I know the school can see what I am doing online when I use the school computers/iPads, including when I am at home
- I know that if I do not follow the rules then I understand I will not be able to access the school systems
- I always tell an adult/teacher if something online makes me feel unhappy or worried
- I can visit www.thinkuknow.co.uk to learn more about keeping safe online
- I have read and talked about these rules with my parents/carers.

Early Years and KS1 Acceptable Use Poster

Key Stage 2 Pupils (7-11)

Acceptable Use Policy:

KS2 Pupils (7-11)

I understand that the Whinfield Primary 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 do not use any personal devices within the school setting.
- Any device should be given to a teacher for safe storage whilst I am in 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 Whinfield Primary School devices for school work unless I have permission otherwise.
- I know that I am not allowed on personal email, social networking sites or instant messaging in school.

- If I need to learn online at home, I will follow the Whinfield Primary School Remote Learning AUP as detailed at the end of this policy.

Trust

- I know that not everything or everyone online is honest or truthful.
- I will check content on other 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 know that being responsible means that I should not look for bad language, inappropriate images or violent or unsuitable games, and that if I accidently come across any of these I should report it to a teacher or adult in school or a parent or carer at home.
- 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 Whinfield Primary School devices and systems are monitored to help keep me safe, including when I use them at home.
- I can visit www.thinkuknow.co.uk and www.childline.org.uk to learn more about being safe online.
- I know that if I do not follow the school rules then I will not be allowed to use devices.
- I have read and talked about these rules with my parents/carers.

Tell

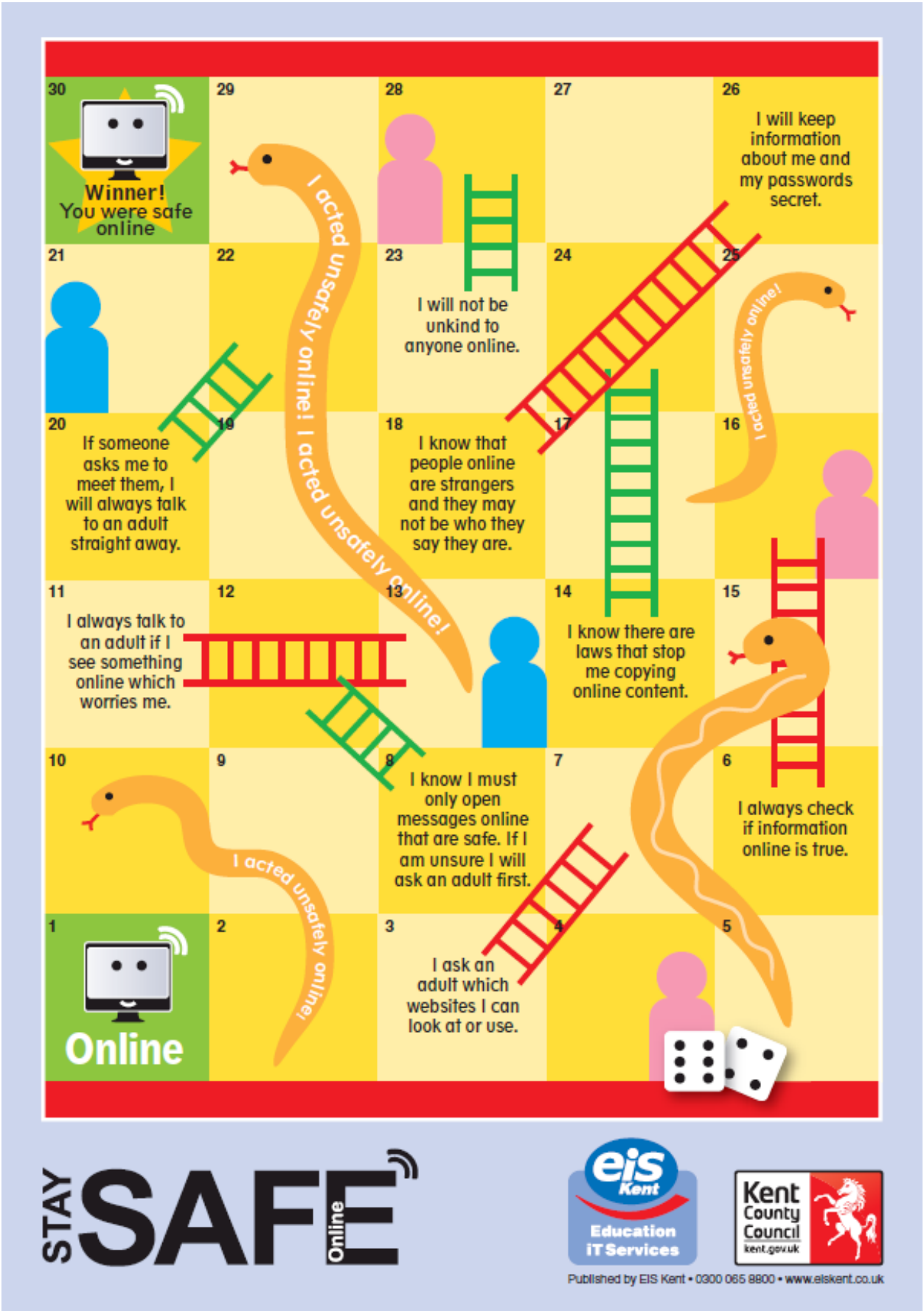
- If I see anything online that I should not or that makes me feel worried or upset, I will minimise the page and tell an adult straight away.

- 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.

- 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.

KS2 Acceptable Use Posters



Whinfield Primary School

STAY SMART! online ONLINE Online Online

I must respect the school's systems and equipment. If I can not be responsible I will lose the right to use them.

RESPONSIBILITY

I must check the reliability of online content, in case it is untrue.

Privacy

I will keep my password and personal information secret.

I know I must always check that my privacy settings are confidential.

I know that my internet use is monitored to protect me.

I am aware that copyright laws exist.

I know that my online actions may have offline consequences.

I know that it can be a criminal offence to hack accounts and systems or to send threatening and offensive messages.

I will always think before I post as once I upload content it can become public and difficult to delete.

I will not use technology to be unkind to people.

REPORT

I know that people online are not always who they say they are. I will always talk to an adult before meeting any online contacts.

If anything happens online which makes me feel worried or uncomfortable, I will speak to an adult I trust or visit ***www.thinkyouknow.co.uk***.

eis Kent Education iT Services

Kent County Council kent.gov.uk

Published by EIS Kent • 0300 065 8800 • www.eiskent.co.uk

Acceptable Use Policy for Children with Additional Needs:

Children with Special Educational Needs and Disabilities

(These statements are based on ability levels rather than age)

Children and Young People 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 something I don't like online, I tell a grown up
- I know that if I do not follow the school rules then I will not be allowed to use the school systems.

Children functioning at Levels P7-L1 (Based on Childnet's SMART Rules: www.childnet.com)

Safe

- I ask a grown up if I want to use the computer
- On the internet I don't tell strangers my name
- I know that if I do not follow the school rules then I will not be allowed to use the school systems.

Meeting

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

Accepting

- I don't open emails from strangers.

Reliable

- I make good choices on the computer.

Tell

- I use kind words on the internet
- If I see something I don't like, then I tell a grown up.

Children and Young People functioning at Levels L2-4 (Based on SMART Rules: www.childnet.com)

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 I will not be allowed to use the school systems.

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 don't 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 don't reply, I save the message and show an adult
- If I see something online, I don't like then I tell an adult.

Parents / Carers Acceptable Use Policy:

Parent/Carers Acceptable Use Policy

1. I, with my child, have read and discussed Whinfield Primary School's Learner Acceptable Use of Technology Policy (AUP) and understand that the AUP will help keep my child safe online.

2. I understand that the AUP applies to my child use of school devices and systems on site and at home, and personal use where there are safeguarding and/or behaviour concerns.

3. I am aware that any use of school devices and systems 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 policy states that my child cannot use personal device and mobile technology on site. Any device brought into school will be given to the class teacher to be stored safely.

5. I understand that my child needs a safe and appropriate place to access remote learning if Whinfield Primary School is closed in response to Covid-19. I will ensure my child's access to remote learning is appropriately supervised. When accessing video learning, I will ensure they are an appropriate location (e.g. not in bed) and that they are suitably dressed.

6. I understand that Whinfield Primary 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 on the internet or if my child is using mobile technologies.

7. I, with my child, am aware of the importance of safe online behaviour and will not deliberately upload or add any images, video, sounds or text that could upset, threaten the safety of or offend any member of Whinfield Primary School's community.

8. I understand that Whinfield Primary School will contact me if they have concerns about any possible breaches of the AUP or have any concerns about my child's safety.

9. I will inform Whinfield Primary School or other relevant organisations if I have concerns over my child's or other members of the school communities' 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 will support Whinfield Primary School's online safety approaches. I will use appropriate parental controls and will encourage my child to adopt safe use of the internet and other technology at home, as appropriate to their age and understanding.

12. I know that I can speak to my child's teacher or the Head Teacher if I have any concerns about online safety (e-Safety).

13. I will visit the school website for more information about the school's approach to online safety as well as to access useful links to support both myself and my child in keeping safe online at home

14. I will visit www.thinkuknow.co.uk/parents, www.nspcc.org.uk/onlinesafety, www.internetmatters.org www.saferinternet.org.uk and www.childnet.com for more information about keeping my child(ren) safe online.

15. I will support the school and my child by role modelling safe and positive online behaviour (such as sharing images, text, video and using social media responsibly) and by discussing online safety with them when they access technology at home.

Use of Cloud Systems Permission Form

The school uses Microsoft Office 365 and other learning platforms in Education for pupils and staff. This consent form describes the tools and pupil responsibilities for using these services.

The following services are available to each pupil and hosted by Microsoft Office 365 as part of the school's online presence in Microsoft Office 365 for Education.

- **Mail** - an individual email account for school use managed by the school
- **Calendar** - an individual calendar providing the ability to organize schedules, daily activities, and assignments
- **People** – an address book
- **Share point** – the schools Virtual Learning Environment for sharing information for individual and collaborative website creation tool
- **Tasks** – a to do list
- **Delve** – the ability to search office 365 for particular files
- **News feed** – up to date news
- **Docs** - a word processing, spreadsheet, drawing, and presentation toolset.

Using these tools, pupils collaboratively create, edit and share files and websites for school related projects and communicate via email with other pupils and members of staff. These services are entirely online and available 24/7 from any Internet-connected computer. Examples of student use include showcasing class projects, building an electronic portfolio of school learning experiences, and working in small groups on presentations to share with others. Examples of cloud servers used in school are : Purple Mash, Showbie, Tapesty, Microsoft Office 365 including email, OneDrive and Apple iCloud.

The school believes that use of the tools significantly adds to your child's educational experience and will offer age related training in school.

As part of our terms and conditions we are required to seek your permission for your child to have a Microsoft Office 365 for Education account so that they can access platforms using the cloud:

Use of Cloud Storage Systems – Parental Consent

Child's Name…….. Class……

Parents Name……

Parents Signature……

Date……

This form was originally created and has been kindly shared by the South West Grid for Learning: www.swgfl.org.uk
This form should be used in accordance with DfE Guidance: https://www.gov.uk/government/publications/cloud-software-services-and-the-data-protection-act

Letter for parents/carers

Dear Parent/Carer,

All pupils use computer facilities including Internet access as an essential part of learning, as required by the National Curriculum. Your child will have the opportunity to access a wide range of information and communication technology (ICT) resources. This includes access to:

- Computers, laptops, IPads, Tablet computers and other digital devices
- Internet which may include search engines and educational websites
- School learning platform/intranet/ Microsoft Office 365
- Email
- Games consoles and other games based technologies
- Digital cameras, web cams and video cameras
- Recorders and Dictaphones
- Mobile Phones and Smartphone's

Whinfield Primary School recognise the essential and important contribution that technology plays in promoting children's learning and development and offers a fantastic range of positive activities and experiences. However, we also recognise there are potential risks involved when using online technology and therefore have developed online safety (e-Safety) policies and procedures alongside the school's firewall and safeguarding measures.

The school takes responsibility for your child's online safety very seriously and, as such, we ensure that pupils are educated about safe use of technology and will take every reasonable precaution and supervision to ensure that pupils cannot access inappropriate materials whilst using school equipment. However, no system can be guaranteed to be 100% safe and the school cannot be held responsible for the content of materials accessed through the internet and the school is not liable for any damages arising from use of the school's internet and ICT facilities.

Full details of the school's Acceptable Use Policy and online safety (e-Safety) policy are available on the school website or on request.

We request that all parents/carers support the schools approach to online safety (e-Safety) by role modelling safe and positive online behaviour for their child and by discussing online safety with them whenever they access technology at home. Parents/carers can visit the school website for more information about the school's approach to online safety as well as to access useful links to support both you and your child in keeping safe online at home. Parents/carers may also like to visit www.thinkuknow.co.uk, www.childnet.com, www.nspcc.org.uk/onlinesafety, www.saferinternet.org.uk and www.internetmatters.org for more information about keeping children safe online

Whilst the school monitors and manages technology use in school we believe that children themselves have an important role in developing responsible online behaviours. In order to support the school in developing your child's knowledge and understanding about online safety, we request that you read the attached Acceptable Use Policy with your child and that you and your child discuss the content and return the attached slip. Hopefully, you will also find this Acceptable Use Policy provides you with an opportunity for conversations between you and your child about safe and appropriate use of the technology, both at school and at home.

Should you wish to discuss the matter further, please do not hesitate to contact your child's class teacher or myself.

Early Years/KS1/SEN

We understand that your child is too young to give informed consent on his/ her own; however, we feel it is good practice to involve them as much as possible in the decision making process, and believe a shared commitment is the most successful way to achieve this.

Yours sincerely,
Mrs S Welsh
Headteacher

Parent/Carer Acceptable Use Policy Acknowledgement Form

Pupil / Parents Acceptable Use Policy – Whinfield Primary School Parental Acknowledgment

I, with my child, have read and discussed Whinfield Primary School Pupil Acceptable Use Policy.

I am aware that any internet and computer use using school equipment may be monitored for safety and security reason to safeguard both my child and the school's systems. This monitoring will be proportionate and will take place in accordance with data protection, privacy and human rights legislation.

I, with my child, am aware of the importance of safe online behaviour and will not deliberately upload or add any images, video, sounds or text that could upset, threaten the safety of or offend any member of the school community.

I understand that the school will take all reasonable precautions to ensure that pupils cannot access inappropriate materials but I appreciate that this is a difficult task. I understand that the school will take all reasonable precautions to reduce and remove risks but cannot ultimately be held responsible for the content of materials accessed through the Internet.

I understand that the school will contact me if they have concerns about any possible breaches of the Acceptable Use Policy or have any concerns about my child's safety.

I will inform the school or other relevant organisations if I have concerns over my child's or other members of the school communities' safety online.

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.

I will support the schools e-Safety approaches and will encourage my child to adopt safe use of the internet and digital technologies at home.

Child's Name…… Signed……

Class…… Date……

Parents Name…… Parents Signature……

Letter for Staff / Governors

Please note this letter does NOT replace a Staff AUP

Dear Staff / Governors,

Social media can blur the definitions of personal and working lives, so it is important that all members of staff take precautions in order to protect themselves both professionally and personally online.

Be very conscious of both your professional reputation and that of the school when you are online. All members of staff are strongly advised, in their own interests, to take steps to ensure that their personal information and content is not accessible to anybody who does not or should not have permission to access it. All staff must also be mindful that any content shared online cannot be guaranteed to be "private" and could potentially be seen by unintended audiences which may have consequences including civil, legal and disciplinary action being taken. Ensure that your privacy settings are set appropriately (many sites have a variety of options to choose from which change regularly and may be different on different devices) as it could lead to your content accidentally being shared with others.

Be very careful when publishing any information, personal contact details, video or images etc online; ask yourself if you would feel comfortable about a current or prospective employer, colleague, child in your care or parent/carer, viewing or sharing your content. If the answer is no, then consider if it should be posted online at all. It is very important to be aware that sometimes content shared online, even in jest, can be misread, misinterpreted or taken out of context, which can lead to complaints or allegations being made. Don't be afraid to be yourself online but do so respectfully. Be accountable and do not disclose information, make commitments or engage in activities on behalf of the school unless you are authorised to do so. All staff must be aware that as professionals, we must be cautious to ensure that the content we post online.

If you have a social networking account, it is advised that you do not to accept parents/carers as "friends" and accept that it is not permitted to accept pupils (past or present) as 'friends' on a personal account. You may be giving them access to your personal information and allowing them to contact you inappropriately through unregulated channels. They may also be giving you access to their personal information and activities which could cause safeguarding concerns. Please ONLY use your work provided email address or phone number to contact children and/or parents – this is essential in order to protect yourself as well as the wider community. If you have a pre-existing relationship with a child or parent/carer that may compromise this or have any queries or concerns about this, then please speak with me.

Documents called "Cyberbullying: Supporting School Staff", "Cyberbullying: advice for headteachers and school staff" and "Safer professional practise with technology" are available to download from www.childnet.com, www.e-safety.org.uk and www.gov.uk/government/publications/preventing-and-

tackling-bullying. Staff can also visit or contact the Professional Online safety Helpline www.saferinternet.org.uk/about/helpline for more advice and information on online professional safety.

I would like to remind all staff of our Acceptable Use Policy and the importance of maintaining professional boundaries online. Failure to follow this guidance and the school policy could lead to disciplinary action, so it is crucial that all staff understand how to protect themselves online. Please speak to me if you have any queries or concerns regarding this.

Yours sincerely,
Mrs S Welsh
Headteacher

Whinfield Primary School

Staff / Governors Acceptable Use Policy 2020

As a professional organisation with responsibility for safeguarding, all members of staff are expected to use Whinfield Primary School's 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 learners, 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 Whinfield Primary School's 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 Whinfield 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 Whinfield Primary School's Acceptable Use of Technology Policy (AUP) should be read and followed in line with the school staff code of conduct and remote learning AUP. (***At end of document***)

3. I am aware that this AUP does not provide an exhaustive list; all staff should ensure that technology use is consistent with the Whinfield Primary 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 learners.

5. I understand that any equipment and internet services provided by my workplace is intended for educational use and should only be accessed by members of staff. Reasonable personal use of setting IT systems and/or devices by staff is allowed as we believe that occasional personal use of the settings devices could be considered as beneficial to the development of staff IT skills and can enable staff to maintain a positive work-life balance. However, this is at the setting's discretion and can be revoked at any time.

6. Where I deliver or support remote learning, I will comply with the school remote 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 use a 'strong' password to access school systems.
- I will protect the devices in my care from unapproved access or theft. I will not leave devices visible or unsupervised in public places or in my car overnight.

8. I will respect school system security and will not disclose my password or security information to others.

9. 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 Head Teacher.

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

11. 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.

12. 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.

13. I will not store any personal information on the school setting 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.

14. 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.

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

16. 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 Service and Head teacher as soon as possible.

17. If I have lost any school related documents or files, I will report this to the Head Teacher and school Data Protection Officer as soon as possible.

18. Any images or videos of learners will only be used as stated in the school camera and image use policy

- I understand images of learners must always be appropriate and should only be taken with school provided equipment and taken/published where learners and their parent/carer have given explicit consent.

Classroom Practice

19. I am aware of the expectations relating to safe technology use in the classroom, safe remote learning, and other working spaces as listed in relevant policies.

20. I have read and understood the school/ mobile technology and social media policies.

21. I will promote online safety with the learners 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 learners feel comfortable to 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) as part of planning online safety lessons or activities to ensure support is in place for any learners who may be impacted by the content.
- make informed decisions to ensure any online safety resources used with learners is appropriate.

22. I will report any filtering breaches (such as access to illegal, inappropriate, or harmful material) to the Head teacher and DSL in line with the school child protection policies.

23. 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.

Use of Social Media and Mobile Technology

24. I have read and understood the school policy which covers expectations regarding staff use of mobile technology and social media.

25. I will ensure that my online reputation and use of IT and information systems are compatible with my professional role and in line with the staff code of conduct, when using school and personal systems. This includes my use of email, text, social media and any other personal devices or mobile technology.

- I will take appropriate steps to protect myself online when using social media as outlined in the social media policy.
- I am aware of the school expectations with regards to use of personal devices and mobile technology, including mobile phones as outlined in the mobile technology policy.

- I will not discuss or share data or information relating to learners, staff, school/setting business or parents/carers on social media.
- I will ensure that my use of technology and the internet does not undermine my professional role or interfere with my work duties and is in accordance with the school behaviour policy/code of conduct and the law.

26. My electronic communications with current and past learners 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, video conferencing tool.
- I will not share any personal contact information or details with learners, 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 learners and/or parents/carers.
- If I am approached online by a learner or parents/carer, I will not respond and will report the communication to my line manager and Designated Safeguarding Lead (DSL).
- Any pre-existing relationships or situations that compromise my ability to comply with the AUP will be discussed with the DSL and/or headteacher/ school manager.

27. 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/school manager.

28. 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.

29. 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.

30. 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.

Policy Compliance

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

Policy Breaches or Concerns

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

33. I will report concerns about the welfare, safety, or behaviour of staff to the headteacher/manager, in line with the allegations against staff policy.

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 code of conduct.

35. I understand that if Whinfield Primary 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 code of conduct.

I have read, understood and agreed to comply with Whinfield Primary School's 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)……

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

The School may exercise its right to monitor the use of information systems, including Internet access and the interception of emails in order to monitor policy compliance. Where it believes unauthorised and/or inappropriate use of the school's information system or unacceptable or inappropriate behaviour may be taking place, the School will invoke its disciplinary procedure. If the school suspects that the school system may be being used for criminal purposes, then the matter will be brought to the attention of the relevant law enforcement organisation.

Visitor/Volunteer Acceptable Use Policy

As a professional organisation with responsibility for children's safeguarding, it is important that all members of the community, including visitors and volunteers, are aware of their professional responsibilities when using technology.
This AUP will help Whinfield Primary School ensure that all visitors and volunteers understand the school 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 Whinfield Primary name 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 Whinfield Primary School's AUP should be read and followed in line with the school staff behaviour 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 will ensure that any access to personal data is kept in accordance with Data Protection legislation, including GDPR.

5. I understand that I am only allowed to take images or videos of learners in line with the school camera and image use policy.

Classroom Practice

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

7. Where I deliver or support remote learning, I will comply with the school remote learning AUP.

8. I will support staff in reinforcing safe behaviour whenever technology is used on site and I will promote online safety with the children in my care.

9. I will immediately report any filtering breaches (such as access to illegal, inappropriate, or harmful material) to the Designated Safeguarding Lead (DSL) in line with the school child protection policy.

10. 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 Social Media and Mobile Technology

11. I have read and understood the school policy which covers expectations regarding staff use of social media and mobile technology.

12, 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 online safety/social media policy
- I will not discuss or share data or information relating to learners, 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 and the law.

13. My electronic communications with learners, 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 this will be discussed with the DSL and headteacher.

14. 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 Designated Safeguarding Lead and the headteacher.

15. 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.

16. 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.

17. 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.

Policy Compliance, Breaches or Concerns

18. I understand that Whinfield Primary School may exercise its right to monitor the use of school information systems, including internet access and the interception of emails, to monitor policy compliance and to ensure the safety of learners, staff and visitors/volunteers. This monitoring will be proportionate and will take place in accordance with data protection, privacy, and human rights legislation.

19. I will report and record concerns about the welfare, safety or behaviour of learners or parents/carers to the Designated Safeguarding Lead in line with the school child protection policy.

20. I will report concerns about the welfare, safety, or behaviour of staff to the headteacher, in line with the allegations against staff policy.

21. I understand that if the school believes that if unauthorised and/or inappropriate use, or unacceptable or inappropriate behaviour is taking place online, the school may invoke its disciplinary procedures.

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

I have read and understood and agree to comply with the Visitor /Volunteer Acceptable Use Policy.

Signed: …….. Print Name: …… Date: ……

Accepted by:…… …… Date: ……..

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's 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 ICT use should be consistent with the school ethos, other appropriate policies and the Law.

Please be 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.

The school provides Wi-Fi for the school community and allows access for education use. There is a guest WIFI which has limited access, please contact the school office for the log in details.

1. The use of ICT devices falls under Whinfield Primary School's Acceptable Use Policy, online safety (e-Safety) policy and behaviour policy, data security, safeguarding/child protection, Mobile Phone and Images policy which all students/staff/visitors and volunteers must agree to, and comply with.

2. 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.

3. School owned information systems, including Wi-Fi, must be used lawfully and 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.

4. I will take all practical steps necessary to make sure that any equipment connected to the school's service is adequately secure (such as up-to-date anti-virus software, systems updates).

5. The school's wireless service is not secure, and the school cannot guarantee the safety of traffic across it. Use of the school's 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. For that reason, I expressly agree that I knowingly assume such risk, and further agree to hold the school harmless from any claim or loss arising out of, or related to, any such instance of hacking or other unauthorized use or access into my computer or device.

6. The school accepts no responsibility for any software downloaded and/or installed, e-mail opened, or sites accessed via the school's 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.

7. The school accepts no responsibility regarding the ability of equipment, owned by myself, to connect to the school's wireless service.

8. I will respect system security and I will not disclose any password or security information that is given to me. To prevent unauthorised access to systems or personal data, I will not leave any information system unattended without first logging out or locking my login as appropriate.

9. I will not attempt to bypass any of the school's security and filtering systems or download any unauthorised software or applications.

10. My use of the 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.

11. 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.

12. I will report any online safety (e-Safety) concerns, filtering breaches or receipt of inappropriate materials to the Designated Safeguarding Lead, or the Headteacher as soon as possible.

13. If I have any queries or questions regarding safe behaviour online, then I will discuss them with the Headteacher as soon as possible.

14. I understand that my use of the schools Wi-Fi will 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 terminate or restrict usage. If the School suspects that the system may be being used for criminal purposes, then the matter will be brought to the attention of the relevant law enforcement organisation.

I have read and understood and agree to comply with Whinfield Primary School Wi-Fi Acceptable Use Policy.

Signed: …… Print Name: …… Date: ……

Accepted by: …… Print Name: ……

Social Networking Acceptable Use Policy

For Staff / parents / volunteers running school social media accounts
e.g. School online accounts, PTA groups and committees

1. As part of the school's drive to encourage safe and appropriate behaviour in the use of today's technology, I will support the school's approach to online safety (e-Safety). I am aware that social media including Facebook, Twitter offer a public and global communication tool and that any content posted on the site/page/group may reflect on the school, its reputation and services. I will not use the site/page/group to express any personal opinions or create, transmit, display, publish or forward any material that is likely to harass, cause offence, inconvenience or needless anxiety to any other person, or anything which could bring the school into disrepute.

2. I will not disclose information, make commitments or engage in activities on behalf of the school without authorisation from the school Designated Safeguarding Lead or the head teacher. The head teacher or other appropriate member of senior leadership retains the right to remove or approve content posted on behalf of the school. Where it believes unauthorised and/or inappropriate use of the tool using e.g. Facebook, Twitter or unacceptable or inappropriate behaviour may be taking place, the school will exercise the right to ask for the content to be deleted or deactivated.

3. I will ensure that any content posted abides by copyright and intellectual property rights, child protection legislation, privacy and data protection law and other relevant civil and criminal legislation.

4. I will follow the school's policy regarding confidentially and data protection/use of images. I will ensure that I have written permission from parents/carers or the school before using any images or videos which include members of the school community. Images of pupils will be taken on school equipment by the school and in accordance with the school image policy. Images which include pupils will only be uploaded by the school and these will be for the sole purpose of inclusion on school Facebook, Twitter and will not be forwarded to any other person or organisation.

5. I will promote online safety in the use of. Facebook and Twitter and will help to develop a responsible attitude to safety online and to the content that is accessed or created. I will ensure that the communication has been appropriately risk assessed and approved by a member of the senior leadership team / designated Safeguarding Lead / Headteacher prior to use.

6. I will set up a specific account/profile using a school provided email address to administrate the account /site and I will use a strong password to secure the account. Personal social networking accounts / email addresses must not be used. The school Designated Safeguarding Lead and/or school management team will have full admin rights to the account.

7. Where school believes unauthorised and / or inappropriate use of the accounts/site or unacceptable or inappropriate behaviour may be taking place, the school will exercise the right to ask for the content to be deleted or deactivated.

8. I will ensure that the content and channel is suitable for the audience and will be sensitive in the tone of language used and will ensure content is written in accessible plain English.

9. I will report any accidental access or receipt of inappropriate materials or inappropriate comments to the Designated Safeguarding Lead and/or head teacher immediately.

10. I will ensure that the Facebook and Twitter accounts are moderated on a regular basis as agreed with the Designated Safeguarding Lead and/or head teacher.

11. I have read and understood the school online safety (e-Safety) policy which covers the requirements for safe ICT use, including using appropriate devices and the safe use of social media. I have ensured that the site has been suitably risk assessed and this use has been agreed by the head teacher.

12. If I have any queries or questions regarding safe and acceptable practise online, I will raise them with the Designated Safeguarding Lead or the head teacher.

I have read and understood and agree to comply with the School Parent Association Social Networking Acceptable Use policy.

Signed: …… Print Name: …… Date: ……

Accepted by: …… Print Name: …… Date:……

Whinfield Primary School's Staff Remote Learning AUP

The Remote Learning Acceptable Use Policy (AUP) is in place to safeguarding all members of Whinfield Primary School community when taking part in remote learning following any isolation period, full or partial school closures.

Leadership Oversight and Approval

1. Remote learning will operate through a virtual classroom that will include online assignments, links to other sites school subscribes to, videos and real time teaching. Our virtual classroom will be Showbie.

- Showbie, Tapestry and Microsoft teams have been assessed and approved by the headteacher.

2. Staff will only use school managed or specific, approved professional accounts with learners and parents/carers.
- Use of any personal accounts to communicate with learners and/or parents/carers is not permitted.

- Any pre-existing relationships or situations which mean this cannot be complied with will be discussed with the Designated Safeguarding Lead (DSL).

- Staff will use work provided equipment where possible e.g. a school/setting laptop, tablet, or other mobile device.

3. Online contact with learners and/or parents/carers will not take place outside of the operating times of 8.30a.m. – 4.30p.m.

4. All remote lessons will be formally timetabled; a member of SLT, DSL and/or head of department is able to drop in at any time.

5. Live streamed remote learning sessions will only be held with approval and agreement from the headteacher or a member of SLT.

Data Protection and Security

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

.

7. All remote learning and any other online communication will take place in line with current school confidentiality expectations as outlined in the Code of Conduct.

8. All participants will be made aware that Showbie and Microsoft teams can record activity.

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 Whinfield Primary School community will be given access to Showbie and Microsoft teams

11. Access to Showbie and Microsoft teams will be managed in line with current IT security expectations as outlined in the **Staff AUP policy.**

Session Management

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

13. Appropriate privacy and safety settings will be used to manage access and interactions.

14. When live streaming with learners:

- contact will be made via learners' **school** provided email accounts **and/or** logins.
- staff will **mute/disable** learners' videos and microphones unless allowed under staff control at specific times. This is likely to vary based on age and ability of learners.

15. Live 1 to 1 sessions will only take place with approval from the **headteacher/a member of SLT**. A pre-agreed **invitation/email** detailing the session expectations will be sent to those invited to attend.

- Access links should not be made public or shared by participants.
- Learners **and/or** parents/carers should not forward or share access links.
- If learners/parents/carers believe a link should be shared with others, they will discuss this with the member of staff running the session first.
- Learners 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.
- Alternative approaches **and/or** access will be provided to those who do not have access.

Behaviour Expectations

16. Staff will model safe practice and moderate behaviour online during remote sessions as they would in the classroom.
17. 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.**
- **Attendees cannot record events for their own use.**

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

19. When sharing videos and/or live streaming, participants are required to:

- **wear appropriate day dress, ensuring torsos are fully covered.**
- **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.**
- **Notifications are turned off so not popping up whilst screen sharing with learners**

20. 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

21. Participants are encouraged to report concerns during remote and/or live streamed sessions:
- Pupils are encouraged to report concerns to the member of staff running the session or to tell a parent/carer etc.

22. 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 DSL and the headteacher.

23. 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.

24. Sanctions for deliberate misuse may include: restricting/removing use or the contacting of police if a criminal offence has been committed.

25. Any safeguarding concerns will be reported to the Designated Safeguarding Lead, in line with our child protection policy.

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

Staff Member Name: ……

Date……

Whinfield Primary School Learner Remote Learning AUP

I understand that:

1.

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

2. Only members of Whinfield Primary School community can access Showbie and Microsoft Teams

- I will only use my school provided email accounts and/or login to access remote learning.
- I will use privacy settings as set up by the school.
- 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 learning I will behave as I would in the classroom. This includes:

- Using appropriate language.
- Not taking or recording images/content without agreement from the teacher and/or those featured.
- Not speaking over the teacher or other students.
- Respecting other opinions.
- Raising hands to ask questions.

4. When taking part in live sessions I will:

- Mute my video and microphone unless otherwise asked by my teacher.
- wear appropriate day clothing, covering all of my torso 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.
- Attend lessons in a shared/communal space or room with an open door and/or where possible when I can be supervised by a parent/carer or another appropriate adult.

5. If I am concerned about anything that takes place during remote learning, I will:

- report my concerns to the member of staff running the session or tell a parent/carer.

6. I understand that inappropriate online behaviour or concerns about my safety during remote learning will be taken seriously. This could include:

- restricting/removing access, following the school's Behaviour Policy, informing parents/carers, contacting police if a criminal offence has been committed.

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

Name…… Signed……

Class…… Date……

Parent/Carers Name…… (*If appropriate*)

Parent/Carers Signature…… (*If appropriate*)

Date……