<insert name of school>

Acceptable Use Policy Statements for Parent/Carers

- I have read and discussed the Acceptable Use Policy for Children (attached) with my child.
- I know that my child will receive online safety (e-Safety) education to help them understand the importance of safe use of technology and the internet, both in and out of school.
- I am aware that any internet and computer use using school equipment may be monitored for safety and security reasons and to safeguard both my child and the school's systems. This monitoring will take place in accordance with data protection and human rights legislation.
- 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 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 Internet facilities.
- I understand that if the school has any concerns about my child's safety online, either at school or at home, then I will be contacted.
- I understand that if my child does not abide by the school Acceptable Use Policy for Children then sanctions will be applied in line with the school's behaviour and anti-bullying policy. If the school believes that my child has committed a criminal offence then the Police will be contacted
- I, together with my child, will support the school's approach to online safety (e-Safety) 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 know that I can speak to the school Online Safety (e-Safety) Coordinator, my child's teacher or the Head Teacher if I have any concerns about online safety (e-Safety).
- I will visit the school website <***Insert School Website Address***> 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.
- 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.
- I will support the school and my child by role modelling safe and positive online behaviour (such as sharing images, text and video responsibly) and by discussing online safety with them when they access technology at home.

I have read the Parent Acceptable Use Policy.

Child's Name…… Class……..……

Parent's Name……....Parent's Signature……

Date……

<insert name of school>

Staff Acceptable Use Policy 2017

As a professional organisation with responsibility for children's safeguarding it is important that all staff take all possible and necessary measures to protect data and information systems from infection, unauthorised access, damage, loss, abuse and theft. All members of staff have a responsibility to use the school's computer system in a professional, lawful, and ethical manner. To ensure that members of staff are fully aware of their professional responsibilities when using Information Communication Technology and the school systems, they are asked to read and sign this Acceptable Use Policy.

This is not an exhaustive list and all members of staff are reminded that ICT use should be consistent with the school ethos, other appropriate school policies, relevant national and local guidance and expectations, and the Law.

1. I understand that Information Systems and ICT include networks, data and data storage, online and offline communication technologies and access devices. Examples include laptops, mobile phones, tablets, digital cameras, email and social media sites**.**

2. School owned information systems must be used 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.

3. I understand that any hardware and software provided by my workplace for staff use can only be used by members of staff and only for educational use. 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.

4. I will respect system security and I will not disclose any password or security information. I will use a 'strong' password (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 and is changed regularly. More information on using strong passwords is found on the school KLZ site.

5. I will not attempt to install any purchased or downloaded software, including browser toolbars, or hardware without permission from the system manager.

6. I will ensure that any personal data of pupils, staff or parents/carers is kept in accordance with the Data Protection Act 1998 and the General Data Protection Regulation 2018. This means that 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 (only within countries or sites with suitable data protection controls that meet the EU and UK regulations) or accessed remotely (e.g. via VPN). Any data which is being removed from the school site (such as via email or on memory sticks or CDs) will be encrypted by a method approved by the school. Any images or videos of pupils will only be used as stated in the school image use policy and will always take into account parental consent.

7. I will not keep or access professional documents which contain school-related sensitive or personal information (including images, files, videos, emails etc.) on any personal devices (such as laptops, digital cameras, mobile phones), unless they are suitably secured and encrypted. Where possible I will use the school learning platform KLZ to upload any work documents and files in a password protected environment or via VPN. I will protect the devices in my care from unapproved access or theft.

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

9. I will respect copyright and intellectual property rights.

10. I have read and understood the school Online Safety (e-Safety) Policy which covers the requirements for safe ICT use, including using appropriate devices, safe use of social media websites and the supervision of pupils within the classroom and other working spaces.

11. I will report all incidents of concern regarding children's online safety to the Designated Safeguarding Lead and/or the Online Safety Coordinator as soon as possible. I will report any accidental access, receipt of inappropriate materials, filtering breaches or unsuitable websites Designated Safeguarding Lead and/or the Online Safety Coordinator and/or the designated lead for filtering as soon as possible.

12. I will not attempt to bypass any filtering and/or security systems put in place by the school. If I suspect a computer or system has been damaged or affected by a virus or other malware, or if I have lost any school related documents or files, then I will report this to the ICT Technician as soon as possible.

13. 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 at all times. All communication will take place via school approved communication channels e.g. via a school provided email address or telephone number and not via personal devices or communication channels e.g. personal email, social networking or mobile phones. Any pre-existing relationships or situations that may compromise this will be discussed with the Senior Leadership team and/or Headteacher.

14. I will ensure that my online reputation and use of ICT and information systems are compatible with my professional role, whether using school or personal systems. This includes the use of email, text, social media/networking, gaming and any other devices or websites. I will take appropriate steps to protect myself online and will ensure that my use of ICT and internet will not undermine my professional role, interfere with my work duties and will be in accordance with the school AUP and the Law.

15. I will not 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 my professional role, the school, Potential in Everyone Academy Trust or the County Council, into disrepute.

16. 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.

17. If I have any queries or questions regarding safe and professional practise online either in school or off site, then I will raise them with the Designated Safeguarding Lead and/or the Online Safety Coordinator or the Headteacher.

18. I will familiarise myself with the Online Safety Policy Appendices as they are published to staff. Notification of any changes to policy will be made in the announcement section of KLZ. Policies and Appendices are available in the Policies folder in the staffroom as well as on KLZ.

19. I understand that my use of the information systems, Internet and email may be monitored and recorded to ensure policy compliance.

The School may exercise its right to monitor the use of information systems, including Internet access and the interception of e-mails in order to monitor compliance with this Acceptable Use Policy and the School's Data Security Policy. Where it believes unauthorised and/or inappropriate use of the service'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 system may be being used for criminal purposes or for storing unlawful text, imagery or sound, the matter will be brought to the attention of the relevant law enforcement organisation.

I have read and understood and agree to comply with the Staff Acceptable Use Policy.

Signed: …….... Print Name: …… Date: ……

Accepted by: …… Print Name: ……..

<insert name of school>

Visitor/Volunteer Acceptable Use Policy

As a professional organisation with responsibility for children's safeguarding it is important that all members of the community are fully aware of their professional responsibilities and read and sign this Acceptable Use Policy. This list is not exhaustive, and visitors/volunteers are reminded that ICT use should be consistent with the school ethos, other appropriate school policies, relevant national and local guidance and expectations, and the Law.

1. I will ensure that any personal data of pupils, staff or parents/carers is kept in accordance with the Data Protection Act 1998 and the General Data Protection Regulation 2018. Any data which is being removed from the school site (such as via email or on memory sticks or CDs) will be encrypted by a method approved by the school. If I am permitted access to any images or videos of pupils I will only use them as stated in the school image use policy and will always take into account parental consent

2. I have read and understood the school online safety (e-Safety) policy which covers the requirements for safe ICT use, including using appropriate devices, safe use of social media websites and the supervision of pupils within the classroom and other working spaces.

3. I will follow the school's policy regarding confidentiality, data protection and the use of images and will abide with copyright and intellectual property rights, child protection legislation, privacy and data protection law, GDPR and other relevant civil and criminal legislation.

4. 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 at all times. All communication will take place via school approved communication channels e.g. via a school provided email address or telephone number and not via personal devices or communication channels e.g. personal email, social networking or mobile phones. Any pre-existing relationships or situations that may compromise this will be discussed with the Senior Leadership team and/or Head Teacher.

5. My use of ICT and information systems will be compatible with my role within school. This includes the use of email, text, social media, social networking, gaming, web publications and any other devices or websites. I will take appropriate steps to protect myself online and my use of ICT will not interfere with my work duties and will always be in accordance with the school AUP and the Law

6. I will not 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 my professional role, the school, the Potential in Everyone Academy Trust or the County Council, into disrepute.

7. I will promote online safety with the children in my care and will help them to develop a responsible attitude to safety online, system use and to the content they access or create.

8. If I have any queries or questions regarding safe and professional practise online either in school or off site, then I will raise them with the Designated Safeguarding Lead/ Head Teacher.

9. I will report any incidents of concern regarding children's online safety to the Designated Safeguarding Lead as soon as possible.

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

Signed: …….... Print Name: …… Date: ……..

Accepted by:…… ……Date: ……..

<insert name of school>

WiFi Acceptable Use Policy

For those using school WiFi

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 schools boundaries and requirements when using the school WiFi 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.

1. The use of ICT devices falls under ***<Insert School Name>*** School's Acceptable Use Policy, online safety (e-Safety), policy and behaviour and safeguarding/child protection policies 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 WiFi, 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 schools 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 unauthorised 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 security and filtering systems or download any unauthorised software or applications.

10. The school provides WiFi for the school community and authorised visitors. My use of the school WiFi 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, the Online Safety (e-Safety) Coordinator and/or the designated lead for filtering as soon as possible.

13. If I have any queries or questions regarding safe behaviour online then I will discuss them with the Online safety (e-Safety) Coordinator or the Head Teacher.

14. I understand that my use of the school's internet will be monitored and recorded to ensure policy compliance in accordance with privacy and data protection and GDPR legislation. If the schools suspects that unauthorised and/or inappropriate use or unacceptable or inappropriate behaviour may be taking place, then the school will 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 <insert school name> WiFi Acceptable Use Policy.

Signed: ……..... Print Name: …… Date: ……

Accepted by: …….…….. Print Name: ……..……