Tunbury Primary School

Acceptable Use Policies

Internet Policy Document

Created: March 2017
To be reviewed: March 2018

Pupils Acceptable Use Policy - Early Years and KS1 (0-7)

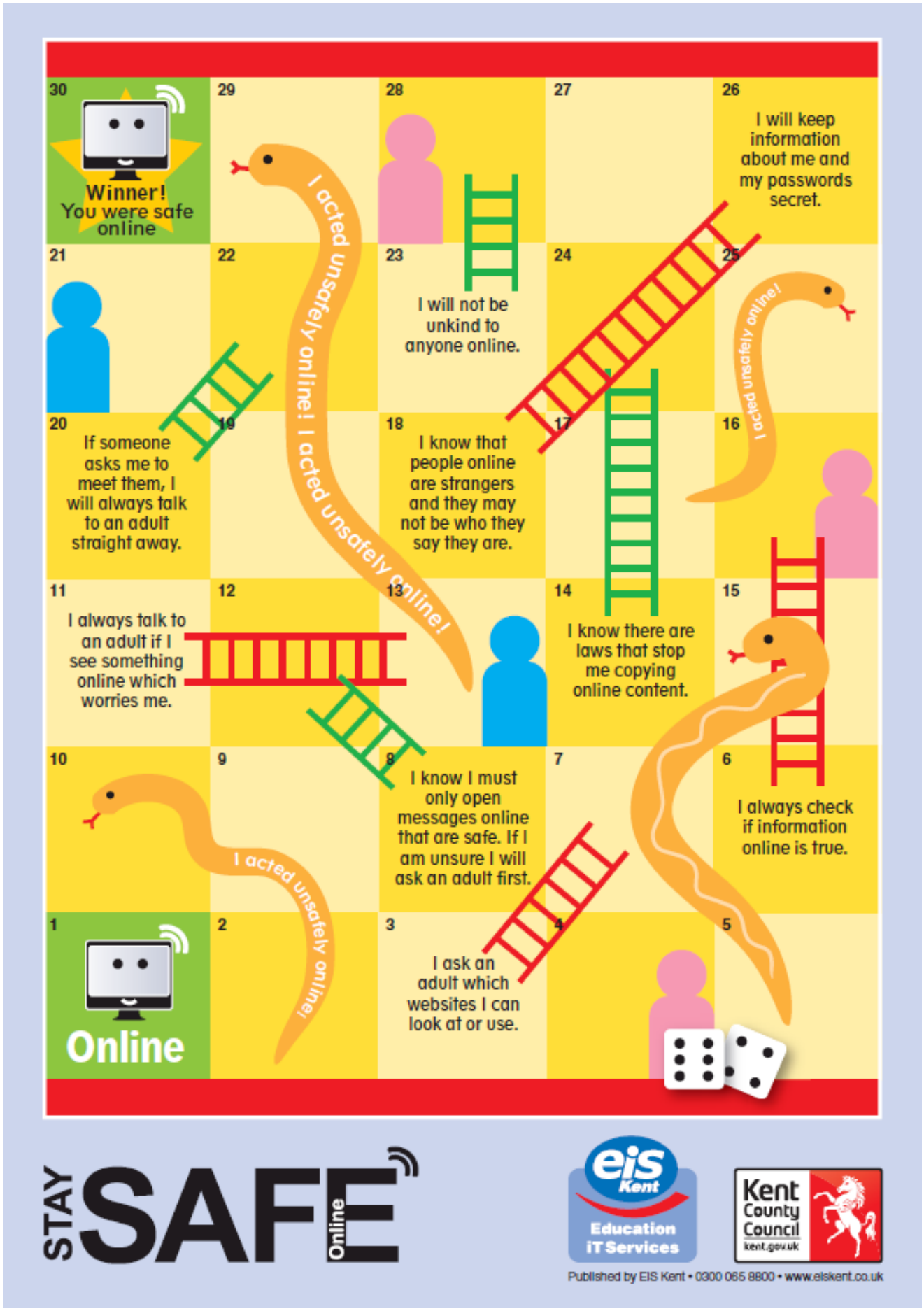
- I only use the internet when an adult is with me.
- I only click on links and buttons when I know what they do.
- I do not share personal information and passwords with other people online.
- I only send messages online which are polite and friendly.
- I know the school can see what I am doing online.
- In school I will only use my own password to use the computers in school and I will not let anyone else use this password.
- In school I will only use the numbered iPad that my teacher tells me to.
- I will tell an adult if someone else tries to use my password or numbered iPad in school.
- I know that if I do not follow the rules then:
    - My Class Teacher will speak to me about my behaviour and remind me of why the rules need to be followed if we are to keep safe online.
    - My Class Teacher will also speak to my parents so that they too can work with the school to ensure that I understand the rules and keep safe when using computers and iPads.
    - If, after my teacher has spoken to me, I continue to break the rules I will not be allowed to use the computers and iPads for the remainder of the lesson.
    - If I have repeatedly broken the rules and as a consequence missed a lesson, I will be allowed to use the computers and iPads in following lessons and I will be expected to follow the rules.
- I have read and talked about these rules with my parents/carers.
- I always tell an adult/teacher if something online makes me feel unhappy or worried.
- I can visit www.thinkuknow.co.uk , https://www.nspcc.org.uk/preventing-abuse/keeping-children-safe/online-safety/ or www.childnet.com to learn more about keeping safe online.

Early Years and KS1 Acceptable Use Poster

Pupils Acceptable Use Policy - KS2 Pupils (7-11)

- 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 my school computers for school work unless I have permission otherwise.
- I will always log off when I have finished using the computer or device.
- I keep my personal information safe and private online.
- If, for any reason, I need to bring my mobile phone into school I know that it is to be handed in to the office and then collected at the end of the school day.
- I do not use my mobile phone during the school day or on the school grounds.
- I know that I will be able to use the internet in school, for a variety of reasons, if I use it responsibly. However, I understand that if I do not, I may not be allowed to use the internet at school.
- I know that not everything or everyone online is honest or truthful and 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, image or text I use.
- I only talk with and open messages from people I know (that I have met) and I only click on links if I know they are safe.
- I always talk to an adult if I'm not sure about something or if something happens online that makes me feel worried or frightened.
- I only send messages which are polite and friendly.
- I will keep my passwords safe and not share them with anyone.
- I will not access or change other people's files or information.
- 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 will only post pictures or videos on the Internet if they are appropriate and if I have permission.
- I will only change the settings on the computer if a teacher/technician has allowed me to.
- I understand that the school's internet filter is there to protect me, and I will not try to bypass it.
- 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.
- I know that my use of school devices/computers and Internet access will be monitored.
- If I bring in memory sticks / CD ROMs from outside of school I will always give them to my teacher so they can be checked for viruses and content, before opening a file.
- If I get unpleasant, rude or bullying emails or messages I will report them to a teacher or other adult. I will not delete them straight away, but instead, keep them so I can show them to the person I am reporting it to.
- I will always be myself and not pretend to be anyone or anything I am not. I know that posting anonymous messages or pretending to be someone else is not allowed.
- In school I will only use my own password to use the computers in school and I will not let anyone else use this password.
- In school I will only use the numbered iPad that my teacher tells me to.
- I will tell an adult if someone else tries to use my password or numbered iPad in school.
- I know that if I do not follow the rules then:
    - My Class Teacher will speak to me about my behaviour and remind me of why the rules need to be followed if we are to keep safe online.
    - My Class Teacher will also speak to my parents so that they too can work with the school to ensure that I understand the rules and keep safe when using computers and iPads.
    - If, after my teacher has spoken to me, I continue to break the rules I will not be allowed to use the computers and iPads for the remainder of the lesson.
    - If I have repeatedly broken the rules and as a consequence missed a lesson, I will be allowed to use the computers and iPads in following lessons and I will be expected to follow the rules.
- If I see anything online that I shouldn't or that makes me feel worried or upset then I will minimise the page and tell an adult straight away.
- I have read and talked about these rules with my parents/carers.
- If I am aware of anyone being unsafe with technology then I will report it to a teacher.
- I can visit www.thinkuknow.co.uk and www.childline.org.uk to learn more about keeping safe online.

KS2 Acceptable Use Poster



Parent/Carer/Pupil Acceptable Use Policy

- I have read and discussed the Acceptable Use Policy (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 schools 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 if the school has any concerns about any possible breaches of the Acceptable Use Policy or 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 then sanctions will be applied in line with the schools behaviour policy. If the school believes that my child has committed a criminal offence then the Police will be contacted.
- 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, together with my child, will support the school's approach to online safety (e-Safety) and will not 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 know that I can speak to the school Online Safety (e-Safety) Coordinator (Angela Carpenter), my child's teacher or the Head Teacher if I have any concerns about online safety (e-Safety).
- I will visit the school website (http://tunbury.kent.sch.uk/) 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 will support the schools e-Safety approaches and will encourage my child to adopt safe use of the internet and digital technologies at home.

Parent/carer's permission

I have read the Parent/Carer and Pupil Acceptable Use Policies and give permission for my child to access the Internet on the terms set out above.

Signed ……...

Print name ……

Date ……

Pupil's agreement

I agree to follow the Pupils Acceptable Use Policy.

Signed ……...

Print name ……

Date ……

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 and iPads
- Internet which may include search engines and educational websites
- School learning platform/intranet
- Games consoles and other games based technologies
- Digital cameras and video cameras

Tunbury Primary school recognises 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 schools 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 to ensure that pupils cannot access inappropriate materials whilst using school equipment. The children are only to use the laptops, computers and iPads when supervised by a member of teaching staff. The children have their own specific passwords with which they must login to use the computers and iPads and which they must not share with others. The children are given numbered iPads to use and the number of each iPad used is logged against the user's name. A company called EIS regularly come into school and make sure that the systems that the children are using are filtered. EIS also keep a record of all the children's online usage each week. All these measures enable us to closely monitor internet usage and ensure that it is as safe as it can be. 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 schools 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 (http://tunbury.kent.sch.uk/) or on request.

We request that all parents/carers support the school's 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 (http://tunbury.kent.sch.uk/) 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 the school online safety Coordinator (Angela Carpenter) or myself.

Yours sincerely,

Miss E McIntosh
Head Teacher

Dear Staff,

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. All staff must be aware that as professionals, we must be cautious to ensure that the content we post online does not bring the school or our professional role into disrepute.

If you have a social networking account, it is advised that you do not to accept pupils (past or present) or their parents/carers 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 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 to the Online safety (e-Safety) and Designated Safeguarding Lead (Angela Carpenter).

Documents called "Cyberbullying: Supporting School Staff", "Cyberbullying: advice for headteachers and school staff" and "Safer professional practise with technology" can be found in the staff admin area and can be used to help you consider how to protect yourself online. Please photocopy them if you want or download the documents directly 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 your line manager, the Designated Safeguarding Lead (Angela Carpenter) or myself if you have any queries or concerns regarding this.

Yours sincerely,

Miss E McIntosh
Head Teacher

Staff Acceptable Use Policy 2016

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 – The school advises that passwords are updated at least yearly.

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. 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 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 (Angela Carpenter) who is also the Online Safety Coordinator as soon as possible. I will report any accidental access, receipt of inappropriate materials, filtering breaches or unsuitable websites to the Designated Safeguarding Lead and Online Safety Coordinator (Angela Carpenter) and/or to the designated lead for filtering (Liz MicIntosh) 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 lead/Support Provider (Liane Morgan or the EIS 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 Head Teacher.

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, 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 Online Safety Coordinator (Angela Carpenter) or the Head Teacher.

18. Staff have individual logins which they must use to access the school computers and laptops. These logins are not to be shared with others. Heads of Year have an iPad that they can loan out to all of the staff in their phase. Supply staff will use similarly traceable guest logins. Members of staff will make sure that students do not have access to the staff laptops and computers by login out when they are not present. Staff must go to the Head of Year if they wish to use their designated iPad and the Head of Year must log staff use and report this to the DSL fortnightly. Mobile phones must be switched to silent and stored away from the children and their learning environments and not used during school lesson time.

19. I understand that my use of the school information systems (including any devices provided by the school), school Internet and school email may be monitored and recorded to ensure the safety of children and staff and to ensure policy compliance. This monitoring will be proportionate and will take place in accordance with data protection, privacy and human rights legislation.

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 schools 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.

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

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

Accepted by: ……. Print Name: ……..

Visitor/Volunteer Acceptable Use Policy

For visitors/volunteers and staff who do not access school ICT systems

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 is not an exhaustive list 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 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.

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

3. 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.

4. 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

5. 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, or the County Council, into disrepute.

6. 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.

7. 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 (Angela Carpenter) or the Head Teacher.

8. I will report any incidents of concern regarding children's online safety to the Designated Safeguarding Lead (Angela Carpenter) 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: ……..

Wi-Fi Acceptable Use Policy

For those using school Wi-Fi

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 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 educational and administrative purposes only. All school computers, laptops and iPads can access the Wi-Fi system for the school. Members of SLT solely possess password to access the guest logins for Wi-FI. The School Business Manager and ICT Lead hold the password which enables individuals to login to the school's network system.

1. The use of ICT devices falls under Tunbury Primary school's Acceptable Use Policy, online safety (e-Safety) policy and behaviour 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 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 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 schools 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 (Angela Carpenter), the Online Safety (e-Safety) Coordinator (Angela Carpenter) and/or the designated lead for filtering (Liz McIntosh) 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 (Angela Carpenetr) or the Head Teacher.

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 schools 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 the Tunbury Primary School Wi-Fi Acceptable Use Policy.

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

Accepted by: ……. Print Name: …….

Social Networking Acceptable Use Policy

For parents/volunteers running school/setting social media accounts e.g. 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 PTA+ is a public and global communication tool and that any content posted on the site may reflect on the school, its reputation and services. I will not use the site 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 (Angela Carpenter) or the head teacher. The head teacher retains the right to remove or approve content posted on behalf of the school. Where it believes unauthorised and/or inappropriate use of tools such as PTA+, Facebook, Twitter etc. 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 the school's website and will not be forwarded to any other person or organisation.

5. I will promote online safety in the use of of tools such as PTA+, Facebook, Twitter etc. and will help to develop a responsible attitude to safety online and to the content that is accessed or created.

6. I will set up a specific account/profile using a school provided email address to administrate the site and I will use a strong password to secure the account. The school Designated Safeguarding Lead and/or school management team will have full admin rights to the account.

7. 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.

8. I will report any accidental access or receipt of inappropriate materials or inappropriate comments to the Designated Safeguarding Lead (Angela Carpenter) and/or head teacher immediately.

9. I will ensure that the use of tools such as PTA+, Facebook, Twitter etc. are moderated on a regular basis as agreed with the Designated Safeguarding Lead (Angela Carpenter) and/or head teacher.

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 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.

11. If I have any queries or questions regarding safe and acceptable practise online I will raise them with the Designated Safeguarding Lead (Angela Carpenter) 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: ……..