



# Acceptable Use Policies for Education Settings and their Wider Communities

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

**June 2021**

# Acceptable Use Policy Templates for Education Settings and their Wider Communities

## Guidance for use

This document was written by the Kent e-Safety strategy group and approved by the Kent Safeguarding Children's Board Education Subgroup.

This AUP template is suitable for all educational settings including (but not limited to) schools, early year's settings, Pupil Referral Units, 14-19 settings, alternative curriculum provisions, Children Centre's, Childminders and hospital schools etc. We encourage all education establishments to ensure that their AUP is fit for purpose and individualised for their context. For simplicity we have used the terms 'school' and 'pupils' or 'students' within this document, but stress that its use within other educational settings and beyond are relevant and appropriate.

## Pupils Acceptable Use Policy: Sample Statements

### Statements for 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 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
- I only use my own technology when an adult has said I can
- I know that if I do not follow the rules then: I will lose the right to use the Internet, my parents will be told and I could face other serious consequences
- 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](http://www.thinkuknow.co.uk) to learn more about keeping safe online

# Early Years and KS1 Acceptable Use Poster

Be

1 I only go online with a grown up



2 I am kind online

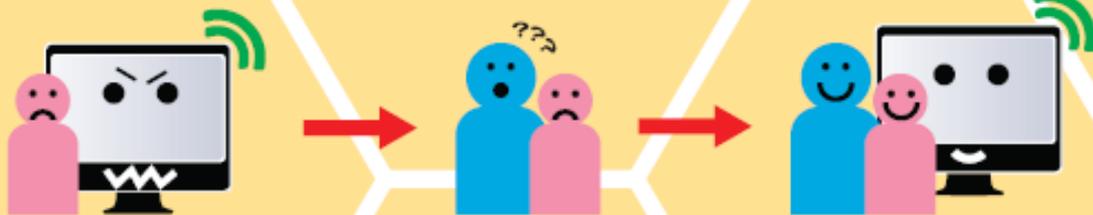


3 I keep information about me safe



Online

4 I tell a grown up if something online makes me unhappy



## Statements for 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 ask my teacher before using my own personal devices/mobile phone
- 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 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 keep my personal information safe and private online
- I will keep my passwords safe and not share them with anyone
- I will not access or change other peoples files or information
- 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 computers and Internet access will be monitored
- All devices and areas visited in school will be used in a way that keeps users safe and does not put them at risk.
- I know that if I do not follow the rules then: I will lose the right to use the Internet, my parents will be told and I could face other serious consequences  
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](http://www.thinkuknow.co.uk) and [www.childline.org.uk](http://www.childline.org.uk) to learn more about keeping safe online

# KS2 Acceptable Use Poster

**30** Winner! You were safe online

**29** I acted unsafely online!

**28** I will not be unkind to anyone online.

**27** I will keep information about me and my passwords secret.

**26**

**25** I acted unsafely online!

**24**

**23** I will not be unkind to anyone online.

**22**

**21**

**20** If someone asks me to meet them, I will always talk to an adult straight away.

**19**

**18** I know that people online are strangers and they may not be who they say they are.

**17**

**16** I acted unsafely online!

**15**

**14** I know there are laws that stop me copying online content.

**13**

**12**

**11** I always talk to an adult if I see something online which worries me.

**10**

**9** I acted unsafely online!

**8** I know I must only open messages online that are safe. If I am unsure I will ask an adult first.

**7**

**6** I always check if information online is true.

**5**

**4**

**3** I ask an adult which websites I can look at or use.

**2**

**1** Online

*I acted unsafely online!*

**STAY SAFE Online**



## Possible Statements for KS3/4/5 Students (11-18)

- I know that school computers and Internet access has been provided to help me with my learning and that other use of technology may not be allowed. If I'm not sure if something is allowed then I will ask a member of staff
- I know that my use of school computers and Internet access will be monitored
- I will keep my password safe and private as my privacy, school work and safety must be protected
- I will write emails and online messages carefully and politely; as I know they could be forwarded or seen by someone I did not intend
- I know that people I meet online may not be who they say they are. If someone online suggests meeting up then I will immediately talk to an adult and will always arrange to meet in a public place, with a trusted adult present
- I know that bullying in any form (on and off line) is not tolerated and I know that technology should not be used for harassment
- I 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 it may be a criminal offence or breach of the school policy to download or share inappropriate pictures, videos or other material online. I also understand that it is against the law to take, save or send indecent images of anyone under the age of 18 and will visit [www.thinkuknow.co.uk](http://www.thinkuknow.co.uk)
- I will protect my personal information online at all times
- I will not access or change other people files, accounts or information
- I will only upload appropriate pictures or videos of others online and when I have permission
- I will only use my personal device/mobile phone in school if I have permission from a teacher
- I will respect other people's information and copyright by giving a reference and asking permission before using images or text from online sources
- I will always check that any information I use online is reliable and accurate
- I will make sure that my internet use is safe and legal and I am aware that online actions have offline consequences
- I will only change the settings on the computer if a teacher/technician has allowed me to
- I know that use of the schools ICT system for personal financial gain, gambling, political purposes or advertising is not allowed
- I understand that the school's Internet filter is there to protect me, and I will not try to bypass it.
- I know that if the school suspect that I am behaving inappropriately with technology, then enhanced monitoring and procedures may be used, such as checking and/or confiscating personal technologies such as mobile phones and other devices
- I know that if I do not follow the AUP then: school sanctions will be imposed according to the behaviour policy  
If I am aware of anyone trying to misuse technology then I will report it to a member of staff
- I will speak to an adult I trust if something happens to either myself or another student which makes me feel worried, scared or uncomfortable
- I will visit [www.thinkuknow.co.uk](http://www.thinkuknow.co.uk) [www.childnet.com](http://www.childnet.com) and [www.childline.org.uk](http://www.childline.org.uk) to find out more about keeping safe online
- I have read and talked about these rules with my parents/carers
- . If I am given permission by a member of staff to use a personal device in school then I will abide by these rules whilst using the device(s) in 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.



## LEGAL

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](http://www.thinkyouknow.co.uk).



# Statements for 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 lose the right to use the Internet, my parents will be told and I could face other serious consequences

## Children functioning at Levels P7-L1 (Based on Childnet's SMART Rules: [www.childnet.com](http://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 lose the right to use the Internet, my parents will be told and I could face other serious consequences

### 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](http://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 lose the right to use the Internet, my parents will be told and I could face other serious consequences

### 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



# Parent/Carers Acceptable Use Policy Statements



- 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 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 then sanctions will be applied in line with the schools 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 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](http://www.thinkuknow.co.uk/parents), [www.nspcc.org.uk/onlinesafety](http://www.nspcc.org.uk/onlinesafety), [www.internetmatters.org](http://www.internetmatters.org) [www.saferinternet.org.uk](http://www.saferinternet.org.uk) and [www.childnet.com](http://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.....

Parents Name.....Parents Signature.....

Date.....

*Note: Please be aware that if parents/carers refuse to sign and agree the AUP then this can cause issues as children will need to use the internet in order to access the curriculum. Schools must have a robust process in place to manage and record parental responses and also to engage with parents who do not respond. Alternatives include highlighting online safety (e-Safety) within the Home School Agreement and a Acknowledgement form for the AUP.*

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

The Tonbridge Federation 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 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. 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 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's ([link](#)) 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](http://www.thinkuknow.co.uk), [www.childnet.com](http://www.childnet.com), [www.nspcc.org.uk/onlinesafety](http://www.nspcc.org.uk/onlinesafety), [www.saferinternet.org.uk](http://www.saferinternet.org.uk) and [www.internetmatters.org](http://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 or myself.

Yours sincerely,  
Headteacher



## Parent/Carer Acceptable Use Policy Acknowledgement Form

### Pupil Acceptable Use Policy –Tonbridge Federation Parental Acknowledgment

I, with my child, have read and discussed The Tonbridge Federation 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 schools systems. This monitoring will take place in accordance with data protection 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 and the school is not liable for any damages arising from use of the Internet facilities.

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, e-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.....

Date.....



# Letter for Students (KS3/4/5)

Dear Student

All students at our school use computer facilities including Internet access as an essential part of learning and fun in today's modern British Society. You will have the opportunity to access a wide range of information and communication technology (ICT) resources. This includes access to:

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

At Hugh Christie we recognise the essential and important contribution that technology plays in promoting your learning and development, both at school and at home. However we also recognise there are potential risks involved when using online technology. The school will take all reasonable precautions to ensure that you are as safe as possible when using school equipment and will work together with you and your family to help you stay safe online.

**At Hugh Christie we want to ensure that all members of our community are safe and responsible uses of technology. We will support you to**

- ☞ Become empowered and responsible digital creators and users
- ☞ Use our school resources and technology safely, carefully and responsibly
- ☞ Be kind online and help us to create a school community that is respectful and caring, on and offline
- ☞ Be safe and be sensible online and always know that you can talk to a trusted adult if you need help

We request that you and your family read the school Acceptable Use Policy and return the attached slip.

Should you have any worries about online safety then you can speak with any member of staff You can also access support through the student support services and via other websites such as [www.thinkuknow.co.uk](http://www.thinkuknow.co.uk) and [www.childline.org.uk](http://www.childline.org.uk)

We look forward to helping you become a positive and responsible digital citizen.

Yours sincerely,

Headteacher

**Pupil Acceptable Use Policy – Hugh Christie Pupil Response**

I, with my parents/carers, have read and discussed the Hugh Christie Pupil Acceptable Use Policy.

Child's Name..... Signed.....

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

Parents Name.....Parents Signature.....

Date.....

# Letter for Staff



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) Co-ordination/ Designated Safeguarding Lead /Manager.

Documents called “Cyberbullying: Supporting School Staff”, “Cyberbullying: advice for headteachers and school staff” and “Safer practise with Technology” are available to download directly from [www.childnet.com](http://www.childnet.com), [www.kelsi.org.uk](http://www.kelsi.org.uk) and [www.gov.uk/government/publications/preventing-and-tackling-bullying](http://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](http://www.saferinternet.org.uk/about/helpline) for more advice and information on online professional safety.

The principles and guidelines below set out the standards of behaviour expected of you as an employee of the school. If you are participating in online activity as part of your capacity as an employee of the school then we request that you:

- Be professional and remember that you are an ambassador for the school. Disclose your position but always make it clear that you do not necessarily speak on behalf of the school.
- Be responsible and honest at all times and consider how the information you are publishing could be perceived
- Be credible, accurate, fair and thorough.
- Always act within the legal frameworks you would adhere to within school, including libel, defamation, confidentiality, copyright, data protection as well as equalities laws.
- 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.
- Always inform your line manager, the designated safeguarding lead and/or the head teacher of any concerns such as criticism or inappropriate content posted online.

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 or myself if you have any queries or concerns regarding this.

Yours sincerely,

Headteacher



# Tonbridge Federation Staff Acceptable Use Policy 2021

**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).
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. 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

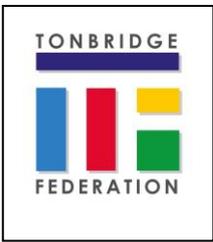
11. I will report all incidents of concern regarding children's online safety to the Designated Safeguarding Lead and/or the Online Safety Coordinator as soon as possible. I will report any accidental access, receipt of inappropriate materials, filtering breaches or unsuitable websites to Designated 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 Support Team 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/or the Online Safety Coordinator or the Head Teacher.
18. 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: .....



# Visitor/Volunteer Acceptable Use Policy

*This AUP may also be useful for 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 confidentiality, 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 or the Head Teacher.
8. 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: .....



# 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.

The school provides WiFi for the school community and allows access for education use only during school hours. Access can be made via password obtained at the office.

1. The use of ICT devices falls under The Tonbridge Federation Acceptable Use Policy, online safety (e-Safety) policy, behaviour policy and safeguarding/child protection 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 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 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 schools internet 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 Tonbridge Federation WiFi Acceptable Use Policy.**

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

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



# Social Networking Acceptable Use Policy



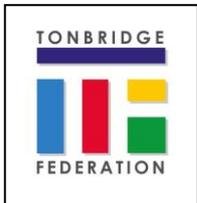
*For parents/volunteers running school/setting social media accounts e.g. PTA groups and committees*

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 when using 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 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 tool using e.g. Facebook, Twitter and will not be forwarded to any other person or organisation.
5. I will promote online safety in the use of tool using e.g. Facebook, Twitter 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 and/or head teacher immediately.
9. I will ensure that the tool using e.g. Facebook, Twitter is moderated on a regular basis as agreed with the Designated Safeguarding Lead 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 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: .....



# Staff Social Networking Acceptable Use Policy



*For use with staff running official school social media accounts*

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 the tool using e.g. Facebook, Twitter is a public and global communication tool and that any content posted 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 and/or the head teacher. The head teacher retains the right to remove or approve content posted on behalf of the school.
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 confidentiality and data protection/use of images. This means I will ensure that the school has written permission from parents/carers before using images or videos which include any members of the school community. Any 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. These will be for the sole purpose of inclusion on tool using e.g. Facebook, Twitter and will not be forwarded to any other person or organisation.
5. I will promote online safety (e-Safety) in the use of tool using e.g. Facebook, 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 senior leadership team/ Designated Safeguarding Lead/head teacher prior to use.
6. I will set up a specific account/profile using a school provided email address to administrate the account/site/page tool using e.g. Facebook, Twitter and I will use a strong password to secure the account. Personal social networking accounts or email addresses are not to be used. The school Designated Safeguarding Lead and/or school leadership team/head teacher will have full admin rights to the tool using e.g. Facebook, Twitter site/page/group.
7. 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.
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 head teacher and/or Designated Safeguarding Lead urgently.
10. I will ensure that the tool using e.g. Facebook, Twitter site/page is moderated on a regular basis as agreed with the school Designated Safeguarding Lead.
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 Social Networking Acceptable Use policy.

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

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