

Small Haven School Acceptable Use Policy

Date	Review Date	Coordinator	Nominated Director
03/09/19	01/9/20	Principal Head	Director of Education

This policy was researched and produced by the SLT in consultation with staff. The designated member responsible for Internet safety in the school is Miss Stacey White (Principal Head).

The aims of this Acceptable Use Policy are to:

- Ensure that pupils benefit from all learning opportunities offered by the computing and internet resources provided by the school in a safe and controlled manner.
- To give pupils clear guidance on safe and acceptable use of these resources.
- Make pupils aware that Internet use in school is a resource. If the resource is abused, then access will be denied.

The ICT Vision is to:

- Develop the learning environment to provide a range of ICT opportunities and tools. This will empower our children to make relevant and safe choices and be flexible as they develop their personalised learning.

General

- Virus protection software is used and updated on a regular basis.
- The ICT Leader is Ross White (supported by BT business service).

Pupils' Access to the Internet

Small Haven School subscribes to NetSupport DNA which contains a wealth of features designed to make School IT management so much easier. Highlights include: automatic discovery of devices; hardware and software inventory; change tracking and software licence management. Building on the flexibility of a single solution for schools, NetSupport DNA also includes energy monitoring; power management; USB endpoint security; printer monitoring; application and internet metering; a flexible alerting suite; and an easy-to-use software distribution module. ESafety and safeguarding are supported with keyword and phrase monitoring to alert schools of any online activity that may place a student at risk; internet monitoring of websites visited; the option for students to report concerns directly to trusted staff – and much more. Small Haven School will normally only allow children to use the Internet when there is a responsible adult present to supervise. Small class numbers and high adult to pupil ratio supports the effectiveness of monitoring pupil's use of computers. However, it is unrealistic to suppose that the teacher's attention will always be directed toward the computer screen. Members of staff will be aware of the potential for misuse, and will be responsible for explaining to pupils, the expectation we have of pupils. NetSupport will also send an immediate warning to both the pupil and the school's DSL where there appears to be inappropriate use of the internet. Teachers will have access to pupils' emails and other Internet related files and will check these on a regular basis to ensure expectations of behaviour are being met, as will NetSupport. The school also operates a strict open DNS filtering system. This restricts access to certain websites, including; gambling sites, post 18 sites, social media sites etc. The school's anti-virus also has network threat protection which protects users against web and network threats.

Expectations of Pupils using the Internet

- All pupils, where possible, are expected to read and agree the Internet Agreement.
- At Small Haven School, we encourage all pupils to be responsible for their own behaviour on the Internet, just as they are anywhere else in school. This includes materials they choose to access, and language they use.

- Pupils using the Internet are expected not to deliberately seek out offensive materials. Should any pupils encounter any such material accidentally, they are expected to report it immediately to a teacher.
- Pupils are expected not to use any rude language in their email communications and contact only people they know or those the teacher has approved. It is forbidden to be involved in sending chain letters.
- Pupils must ask permission before accessing the Internet.
- Pupils will not access social networking sites unless expressly permitted by the school or as part of a specific learning activity.
- Pupils should not access other people's files unless permission has been given.
- Computers should only be used for schoolwork and homework unless permission has been granted otherwise.
- No applications may be downloaded to the school's computers from the Internet or brought in on portable media from home for use in school
- Personal printing is not allowed on the school network.
- No personal information such as phone numbers and addresses should be given out and no arrangements to meet someone made unless this is part of an approved school project.
- The school encourages the use of anti-virus software on machines used at home.
- Pupils consistently choosing not to comply with these expectations will be warned, and subsequently, may be denied access to Internet resources.

School Website

- The website will be regularly checked to ensure that there is no content that compromises the safety of pupils or staff.
- The publications of children's work will be decided by a teacher.
- The school will endeavour to use digital photographs, audio or video clips focusing on group activities. Photographs and video focusing on individual children will not be published on the school website without parental permission.
- The school website will avoid publishing the full names of individuals in a photograph.
- The school will ensure that the image files are appropriately named and will not use pupils' names in image file names if published on the web.

Personal Devices

Pupils may only use their own technology in school as part of a pre-arranged educational activity, with permission from a member of staff and authorised by the teacher/principal head. Inappropriate use is in direct breach of the school's acceptable use policy.

Sanctions

Persistent misuse of the internet by pupils will result in reduced access to the Internet. Misuse of other technologies will result in a complete ban and/or confiscation. Both of these actions will take place for a set period of time agreed by the Principal Head. Parents will always be notified.

No application or services accessed by pupils or their parents may be used to bring the school or its members into disrepute. All users have a responsibility to report any known misuses of technology, including the unacceptable behaviours of others.

KS1 Acceptable Use Poster



1 I only go online with a grown up



2 I am kind online



3 I keep information about me safe



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



KS2 Acceptable Use Poster

The board game grid consists of 30 numbered squares (1-30) arranged in a 6x5 grid. The starting square is 1, and the goal is square 30. The board features several ladders and snakes. The text on the board is as follows:

- Square 1:** Online (with computer icon)
- Square 2:** I ask an adult which websites I can look at or use.
- Square 3:** I know I must only open messages online that are safe. If I am unsure I will ask an adult first.
- Square 4:** I know there are laws that stop me copying online content.
- Square 5:** I always check if information online is true.
- Square 6:** I know that people online are strangers and they may not be who they say they are.
- Square 7:** I will not be unkind to anyone online.
- Square 8:** I always talk to an adult if I see something online which worries me.
- Square 9:** If someone asks me to meet them, I will always talk to an adult straight away.
- Square 10:** I know there are laws that stop me copying online content.
- Square 11:** I know that people online are strangers and they may not be who they say they are.
- Square 12:** I will not be unkind to anyone online.
- Square 13:** I always talk to an adult if I see something online which worries me.
- Square 14:** I know that people online are strangers and they may not be who they say they are.
- Square 15:** I will not be unkind to anyone online.
- Square 16:** I know there are laws that stop me copying online content.
- Square 17:** I always check if information online is true.
- Square 18:** I know that people online are strangers and they may not be who they say they are.
- Square 19:** I will not be unkind to anyone online.
- Square 20:** If someone asks me to meet them, I will always talk to an adult straight away.
- Square 21:** I know that people online are strangers and they may not be who they say they are.
- Square 22:** I will not be unkind to anyone online.
- Square 23:** I always talk to an adult if I see something online which worries me.
- Square 24:** I know that people online are strangers and they may not be who they say they are.
- Square 25:** I will not be unkind to anyone online.
- Square 26:** I will keep information about me and my passwords secret.
- Square 27:** I know that people online are strangers and they may not be who they say they are.
- Square 28:** I will not be unkind to anyone online.
- Square 29:** I always talk to an adult if I see something online which worries me.
- Square 30:** Winner! You were safe online (with computer icon)

Snakes and ladders are placed on the board as follows:

- Snakes:** One from 10 to 4, one from 16 to 8, one from 25 to 12, one from 28 to 15.
- Ladders:** One from 2 to 9, one from 3 to 18, one from 4 to 14, one from 5 to 20, one from 6 to 25, one from 7 to 24, one from 8 to 19, one from 9 to 28, one from 10 to 27, one from 11 to 26, one from 12 to 25, one from 13 to 24, one from 14 to 23, one from 15 to 22, one from 16 to 21, one from 17 to 20, one from 18 to 19, one from 19 to 18, one from 20 to 17, one from 21 to 16, one from 22 to 15, one from 23 to 14, one from 24 to 13, one from 25 to 12, one from 26 to 11, one from 27 to 10, one from 28 to 9, one from 29 to 8.

STAY SAFE Online



KS3/4 Acceptable Use Poster

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.



Use of Photographs and/or Video

Small Haven School uses photographs and/or videos to showcase our pupil's achievements and promote the school.

Small Haven School Pupil Internet & ICT Agreement

Please tick the boxes and sign:

I have read through this agreement with my child and we agree to these safety measures.

I agree to the above and understand that there will be sanctions if the rules are broken.

I consent to photographs and/or videos being used in the following ways:

School Photo Album

School Displays

School Concerts

Exhibitions outside the school

Staff Coursework

Press Releases

School Web Site

Sports Events/Competitions

Signed: (Pupil)

Name of child:

Class:

Signed: (Parent/Carer)

Date:.....

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 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 (Miss White) or my child's teacher if I have any concerns about online safety (e-Safety)
- I will visit the school website (www.smallhavenschool.co.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

'As a parent, I support school safeguarding policies and I will ensure that I monitor my child's use of the internet (including social networking) outside of school. I will act as a positive role model to my child by ensuring that I use social networking sites responsibly.'

I have read the Parent Acceptable Use Policy.

Child's Name..... Class.....

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

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 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

Small Haven School recognise the essential and important contribution that technology plays in promoting children's learning and development and offers a fantastic range of positive activities and experiences. However we also recognise there are potential risks involved when using online technology and therefore have developed online safety (e-Safety) policies and procedures alongside the schools safeguarding measures. The school have effective filtering and monitoring in place via NetSupport DNA, eSafety and safeguarding are supported with keyword and phrase monitoring to alert schools of any online activity that may place a student at risk; internet monitoring of websites visited; the option for students to report concerns directly to trusted staff who flag up immediately any concerns where misuse of a computer is taking place.

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 (www.smallhavenschool.co.uk) 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 (www.smallhavenschool.co.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 Miss Stacey White, Principal Head.

We understand that in the lower school (KS1) your child is too young to give informed consent on his/ her own; however, we feel it is good practice to involve them as much as possible in the decision making process, and believe a shared commitment is the most successful way to achieve this.

Yours sincerely,
Principal Head

Parent/Carer Acceptable Use Policy Acknowledgement Form

Pupil Acceptable Use Policy – Small Haven School Parental Acknowledgment

I, with my child, have read and discussed Small Haven School Pupil Acceptable Use Policy.

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

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

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

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

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

I know that my child will receive online safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.

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

Child's Name..... Signed (if appropriate).....

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

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

Date.....



Sample Letter for Students (KS3/4/5)

Dear

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

At Small Haven School 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. Our easy-to-use software module eSafety and safeguarding are supported with keyword and phrase monitoring to alert us of any online activity that may place a student at risk; internet monitoring of websites are visited; there is an option for you to report concerns directly to trusted staff. Small Haven School will normally only allow children to use the Internet when there is a responsible adult present to supervise. However it is unrealistic to suppose that the teacher's attention will always be directed toward the computer screen. Members of staff will be aware of the potential for misuse, and will be responsible for explaining to pupils, the expectation we have of pupils. Net Support will also send an immediate warning to both the pupil and the school's DSL where there appears to be inappropriate use of the internet. Teachers will have access to pupils' emails and other Internet related files and will check these on a regular basis to ensure expectations of behaviour are being met, as will Net Support.

At Small Haven School 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 Miss White, Principal Head. You can also access support through the school deputy DSL, Tim Catherall, and via other websites such as www.thinkuknow.co.uk and www.childline.org.uk.

We look forward to helping you become a positive and responsible digital citizen.
Yours sincerely,
Principal Head

Pupil Acceptable Use Policy –Small Haven School Pupil Response

I, with my parents/carers, have read and discussed Small Haven school Pupil Acceptable Use Policy.

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

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

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

Date.....

Acceptable Use 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) Coordination/ Designated Safeguarding Lead, Stacey White.

Documents called “Cyberbullying: Supporting School Staff”, “Cyberbullying: advice for headteachers and school staff” and “Safer professional practise with technology” are available to download from www.childnet.com, www.e-safety.org.uk and www.gov.uk/government/publications/preventing-and-tackling-bullying. Staff can also visit or contact the Professional Online safety Helpline www.saferinternet.org.uk/about/helpline for more advice and information on online professional safety.

Additional information for staff regarding online participation on behalf of the School

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 me if you have any queries or concerns regarding this.

Yours sincerely,

Stacey White
Principal Head

Small Haven School Staff Acceptable Use Policy

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, not personal 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 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 Principal Head.
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). Where possible I will use the School server 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/Online Safety Coordinator (Stacey White) 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 the designated lead for filtering (Ross White) 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 lead (Ross White) 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 approved, 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.
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, or the school, 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.
18. 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 will ensure that any personal data of pupils, staff or parents/carers is kept in accordance with the Data Protection Act 1998. 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.
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 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.
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 or Principal Head.
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, 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 (Miss Stacey White) Principal Head.
9. I will report any incidents of concern regarding children’s online safety to the Designated Safeguarding Lead (Miss Stacey White) 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 education use only. Secure individual passwords are given to students and staff, and these are not be shared with others. Passwords are changed with regularity and security around protecting data is taken extremely seriously.

1. The use of ICT devices falls under Small Haven School's Acceptable Use Policy, online safety (e-Safety) policy and behaviour policy, data security & safeguarding/child protection 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 (Miss Stacey White) the Online Safety 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 (Miss Stacey White) Principal Head.
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 Small Haven 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 Facebook & Twitter are 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 (Miss Stacey White) principal head. The principal head retains the right to remove or approve content posted on behalf of the school. Where it believes unauthorised and/or inappropriate use of 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 the school website, Facebook & Twitter and will not be forwarded to any other person or organisation.
5. I will promote online safety in the use of 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 SLT 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 (Miss Stacey White) principal head.
9. I will ensure that Facebook & Twitter is moderated on a regular basis as agreed with the Designated Safeguarding Lead (Miss Stacey White) principal head.
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 principal head.
11. If I have any queries or questions regarding safe and acceptable practise online I will raise them with the Designated Safeguarding Lead (Miss Stacey White) principal head.

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 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 (Stacey White) principal head. The principal head 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 the school website, 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 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/principal head 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 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 (principal head) and school leadership team 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 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 principal head (Designated Safeguarding Lead) urgently.
10. I will ensure that the tool using 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 principal head.
12. If I have any queries or questions regarding safe and acceptable practise online I will raise them with the Designated Safeguarding Lead (Stacey White) principal head.

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: