

Herne Bay Infant School and Seashells Nursery

Acceptable Use Policies



Amended:

Date: September 2019

Approved by the Governing Body:

Date: October 2019

Review:

Date: September 2020

Acting Headteacher:

Date: September 2019

Named Governor with Lead Responsibility: Kate Amos



Herne Bay Infant School and Seashells Nursery

Acceptable Use Policies

Key Details

Designated Safeguarding Lead (s):
Helen Day (Acting Headteacher)
Leigh Bryant (Acting Deputy Head)
Linzi Bradbury (Acting Assistant Head)
Fiona Wood (SENCo)

Named Governor with lead responsibility: (Kate Amos)

Pupils Acceptable Use Policy



- 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 do not bring my own devices into school
- I know that if I do not follow the rules then: I will spend my playtime with a grown up talking about the rules
- I have read and talked about these rules with my parents/carers
- I always tell an adult/teacher if something online makes me feel unhappy or worried
- I can visit www.thinkuknow.co.uk to learn more about keeping safe online

Early Years and KS1 Acceptable Use Poster

Be SAFE Online

- 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

eis Kent
Education IT Services

Kent County Council
kent.gov.uk

Published by EIS Kent • 0900 065 8800 • www.eiskent.co.uk



Parent/Carers Acceptable Use Policy

1. I have read and discussed Herne Bay Infants School and Seashell Nursery Acceptable Use Policy with my child.
2. 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.
3. I am aware that any internet and computer use using school equipment may be monitored for safety and security reasons, to safeguard both my child and the schools' systems. This monitoring will take place in accordance with data protection (including GDPR) and human rights legislation.
4. I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.
5. 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.
6. I understand that if my child does not abide by the school Acceptable Use Policy then sanctions will be applied in line with the school policies including behaviour, online safety and anti-bullying policy. If the school believes that my child has committed a criminal offence then the Police will be contacted.
7. I, together with my child, will support the school's approach to online 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.
8. I know that I can speak to the school Designated Safeguarding Lead Helen Day, Leigh Bryant, Linzi Bradbury, Fiona Wood, Dez Riddler my child's teacher if I have any concerns about online safety.
9. I will visit the school website www.herne-bay.kent.sch.uk for more information about the school's approach to online safety as well as to access useful links to support both myself and my child in keeping safe online at home.
10. I will visit the following websites for more information about keeping my child(ren) safe online:
 - www.thinkuknow.co.uk/parents,
 - www.nspcc.org.uk/onlinesafety
 - www.internetmatters.org
 - www.saferinternet.org.uk
 - www.childnet.com
11. 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, understood and agree to comply with the Herne Bay Infant School and Seashells Nursery 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, iPads and other digital devices
- Internet which may include search engines and educational websites and Learning Platforms
- Digital cameras, web cams and video cameras
- Recorders

Herne Bay Infant School and Seashells Nursery 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 policies and procedures alongside the schools safeguarding measures.

The school takes responsibility for your child's online safety very seriously and, as such, we ensure that pupils are educated about safe use of technology and will take every reasonable precaution to ensure that pupils cannot access inappropriate materials whilst using school equipment. The children are taught how to stay safe digitally as a regular part of the curriculum. Safe Surfers promote digital safety across our school and children are closely supervised when using devices.

However, no system can be guaranteed to be 100% safe and the school cannot be held responsible for the content of materials accessed through the internet and the school is not liable for any damages arising from use of the school's internet and ICT facilities.

Full details of the school's Acceptable Use Policy and online safety policy are available on the school website <http://www.herne-bay.kent.sch.uk/> or on request.

We request that all parents/carers support the schools approach to online 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 <http://www.herne-bay.kent.sch.uk/> for more information about the school's approach to online safety as well as to access useful links to support both you and your child in keeping safe online at home. Parents/carers may also like to visit www.thinkuknow.co.uk, www.childnet.com, www.nspcc.org.uk/onlinesafety, www.saferinternet.org.uk and www.internetmatters.org for more information about keeping children safe online

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

Should you wish to discuss the matter further, please do not hesitate to contact me.

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

Yours sincerely,

Acting Headteacher
Helen Day



Parent/Carer Acceptable Use Policy Acknowledgement Form

Pupil Acceptable Use Policy –Herne Bay Infant School Parental Acknowledgment

I, with my child, have read and discussed **Herne Bay Infant School** Pupil Acceptable Use Policy.

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

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

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

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

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

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

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

Child's Name.....

Class.....

Date.....

Dear Colleague



Social media can blur the definitions of personal and working lives, so it is important that all members of staff take precautions 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 Designated Safeguarding Lead .

Documents called “Cyberbullying: Supporting School Staff”, “Cyberbullying: advice for Headteachers and school staff” and “Safer professional practise with technology” are available in the staffroom to help you consider how to protect yourself online. Please photocopy them if you want or download the documents directly from www.childnet.com, www.e-safety.org.uk and www.gov.uk/government/publications/preventing-and-tackling-bullying. Staff can also visit or contact the Professional Online Safety Helpline www.saferinternet.org.uk/about/helpline for more advice and information on online professional safety.

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

Yours sincerely,
Acting Headteacher
Helen Day

Additional content for staff regarding online participation on behalf 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, 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 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 headteacher of any concerns such as criticism or inappropriate content posted online.

Herne Bay Infant School and Seashells Nursery

Staff Acceptable Use Policy 2019

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 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 one of the Designated Safeguarding Leads Helen Day, Leigh Bryant, Linzi Bradbury, Fiona Wood or Dez Riddler as soon as

possible. I will report any accidental access, receipt of inappropriate materials, filtering breaches or unsuitable websites to Designated Safeguarding Lead

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 Marie Geurts 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.
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 practice online either in school or off site, then I will raise them with the Designated Safeguarding Leads.
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:

Date:



Visitor/Volunteer Acceptable Use Policy

As a professional organisation with responsibility for children's safeguarding it is important that all members of the community are fully aware of their professional responsibilities and read and sign this Acceptable Use Policy. This 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 Data Protection legislation, including GDPR. 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 reflect parental consent. I have read and understood the school online 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 have read and understood the school online 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.
 - All communication will take place via school approved communication channels such as via a school provided email address or telephone number and not via personal devices or communication channels such as via personal email, social networking or mobile phones.
 - Any pre-existing relationships or situations that may compromise this will be discussed with the Designated Safeguarding Lead Helen Day, Leigh Bryant, Linzi Bradbury, Fiona Wood, Dez Riddler.
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 Leads Helen Day, Leigh Bryant, Linzi Bradbury, Fiona Wood or Dez Riddler.
9. I will report any incidents of concern regarding children’s online safety to one of the Designated Safeguarding Leads as soon as possible.
10. I understand that if the school believes inappropriate use or unacceptable behaviour is taking place, the school may invoke its disciplinary procedure. If the school suspects criminal offences have occurred, 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 Visitor /Volunteer Acceptable Use Policy.

Signed: Print Name: 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.

The use of ICT devices falls under Herne Bay Infant School and Seashells Nursery school's Acceptable Use Policy, online safety policy, behaviour policy safeguarding/child protection policy which all students/staff/visitors and volunteers must agree to, and comply with.

1. 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.
2. 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.
3. 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).
4. 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.
5. 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.
6. The school accepts no responsibility regarding the ability of equipment, owned by myself, to connect to the school's wireless service.
7. 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.

8. I will not attempt to bypass any of the school's security and filtering systems or download any unauthorised software or applications.
9. 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.
10. 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.
11. I will report any online safety concerns, filtering breaches or receipt of inappropriate materials to one of the Designated Safeguarding Leads Helen Day, Leigh Bryant, Linzi Bradbury , Fiona Wood, Dez Riddler as soon as possible.
12. If I have any queries or questions regarding safe behaviour online then I will discuss them with the Headteacher.
13. I understand that my use of the schools Wi-Fi will be monitored and recorded to ensure policy compliance in accordance with privacy and data protection legislation. If the school suspects that unauthorised and/or inappropriate use or unacceptable or inappropriate behaviour may be taking place, then the school terminate or restrict usage. If the School suspects that the system may be being used for criminal purposes then the matter will be brought to the attention of the relevant law enforcement organisation.

I have read and understood and agree to comply with Herne Bay Infant School and Seashells Nursery Wi-Fi Acceptable Use Policy.

Signed: Print Name: Date:

Accepted by: Print Name: Date:



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. 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.
2. 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.
3. I will not disclose information, make commitments or engage in activities on behalf of the school without authorisation from the school one of the Designated Safeguarding Lead Helen Day, Leigh Bryant, Linzi Bradbury, Fiona Wood or Dez Riddler. The Headteacher or other appropriate member of senior leadership retains the right to remove or approve content posted on behalf of the school. Where it believes unauthorised and/or inappropriate use of the tool using e.g. Facebook, Twitter or unacceptable or inappropriate behaviour may be taking place, the school will exercise the right to ask for the content to be deleted or deactivated.
4. 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.
5. I will follow the school's policy regarding confidentiality 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 Facebook, Twitter and will not be forwarded to any other person or organisation.
6. 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.
7. 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.
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 one of the Designated Safeguarding Lead Bernadette Lax, Helen Day, Fiona Wood or Dez Riddler.

10. I will ensure that the Facebook, Twitter is moderated on a regular basis as agreed with the Designated Safeguarding Leads.
11. I have read and understood the school online 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 Headteacher.
12. If I have any queries or questions regarding safe and acceptable practise online I will raise them with one of the Designated Safeguarding Leads Helen Day, Leigh Bryant, Linzi Bradbury, Fiona Wood or Dez Riddler.

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

Signed: Print Name: Date:

Accepted by: Print Name: Date:

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. I am aware that Facebook and Twitter are a public and global communication tool and that any content posted may reflect on the school, its reputation and services.
2. 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.
3. I will not disclose information, make commitments or engage in activities on behalf of the school without authorisation from one of the school Designated Safeguarding Leads Helen Day, Leigh Bryant, Linzi Bradbury, Fiona Wood, Dez Riddler. The Headteacher retains the right to remove or approve content posted on behalf of the school.
4. 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.
5. 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 Facebook or Twitter and will not be forwarded to any other person or organisation.
6. I will promote online safety in the use of Facebook and Twitter and will help to develop a responsible attitude to safety online and to the content that is accessed or created. I will ensure that the communication has been appropriately risk assessed and approved by a member of senior leadership team/ Designated Safeguarding Lead/Headteacher prior to use.
7. I will set up a specific account/profile using a school provided email address to administrate the account/site/page Facebook or 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/Headteacher will have full admin rights to the Facebook and Twitter site/page/group.
8. Where it believes unauthorised and/or inappropriate use of Facebook, or Twitter unacceptable or inappropriate behaviour may be taking place, the school will exercise the right to ask for the content to be deleted or deactivated.
9. 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.
10. I will report any accidental access or receipt of inappropriate materials or inappropriate comments to the Headteacher or Designated Safeguarding Lead urgently.

11. I will ensure that the Facebook and Twitter site/page is moderated on a regular basis as agreed with the school Designated Safeguarding Lead.
12. I have read and understood the school online 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 Headteacher.
13. If I have any queries or questions regarding safe and acceptable practise online I will raise them with one of the Designated Safeguarding Lead Helen Day, Leigh Bryant, Linzi Bradbury, Fiona Wood or Dez Riddler.

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: Date: