Briary Primary School

Acceptable Use Policy

Date Reviewed: March 2021
Date Adopted: 25th March, 2021
Date of Next Review: March 2022

At Briary Primary School, we want to ensure that all members of our community are safe and responsible users of technology. We will support our learners to…

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

Early Years and Key Stage 1 (0-6)

- I only use the internet when an adult is with me
- I only click on links and buttons online 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 know that if I do not follow the rules then:
    - The grown-ups that look after me will be informed
    - My use of devices in school and/or access to the internet may be restricted
    - Other sanctions, in line with the school Behaviour Policy may be applied.
- 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

At Briary Primary School, we want to ensure that all members of our community are safe and responsible users of technology. We will support our learners to…

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

Key Stage 2 (7-11)

Safe

- I only send messages which are polite and friendly
- I will only post pictures or videos on the internet if they are appropriate and if I have permission
- I only talk with and open messages from people I know, and I only click on links if I know they are safe
- 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 will protect myself by never telling anyone I meet online my address, my telephone number, my school's name or by sending a picture of myself without permission from a teacher or other adult.

Trust

- I know that not everything or everyone online is honest or truthful
- I 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

Responsible

- I always ask permission from an adult before using the internet
- I only use websites and search engines that my teacher has chosen
- I know that being responsible means that I should not look for bad language, inappropriate images or violent or unsuitable games, and that if I accidently come across any of these I should report it to a teacher or adult in school or a parent or carer at home.
- I will not use my own personal devices/mobile phone in school unless I have specific, written permission to do so.

- If I need to bring my mobile phone to school, I will hand it in to the School Office for safe-keeping on arrival and collect it at the end of the school day. I will not use it on school premises.
- 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 people's files or information
- I will only change the settings on the computer if a teacher/technician has allowed me to
- If I need to learn online at home, I will follow the school remote learning AUP.

Understand

- I know that I will be able to use the internet in school, for a variety of reasons, if I use it responsibly. However, I understand that if I do not, I may not be allowed to use the internet at school.
- I understand that the school's internet filter is there to protect me, and I will not try to bypass it.
- I know that my use of school devices/computers and internet access will be monitored
- I have read and talked about these rules with my parents/carers
- I can visit www.thinkuknow.co.uk and www.childline.org.uk to learn more about keeping safe online
- I know that if I do not follow the school rules then:
    - The grown-ups that care for me will be informed
    - My use of devices and/or access to the internet may be restricted
    - Other sanctions, in line with the school Behaviour Policy may be applied.

Tell

- If I am aware of anyone being unsafe with technology, I will report it to a teacher or other adult in school
- 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
- 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. If I am using a tablet device, I will turn it screen down on a table and tell an adult straight away.

Acceptable Use Policy Agreement Form

Briary Primary School Acceptable Use Policy - Pupil Response

I, with my parents/carers, have read and understood the Acceptable Use Policy (AUP).

I agree to follow the AUP when:

1. I use school systems and devices, both on and offsite
2. I use my own equipment out of the school, in a way that is related to me being a member of the school community, including communicating with other members of the school.

Name……………………………………………. Signed……………………….

Class………………………. Date…………………….

Parent/ Carer's Name…………………………………………........

Parent/ Carer's Signature………………………….

Date…………….

Letter for Parents and Carers

Dear Parent/Carer

All pupils at Briary Primary School, use computer facilities and 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, tablets and other digital devices
- The Internet, which may include search engines and educational sites
- School intranet
- Email
- Digital cameras, webcams and video cameras

Briary Primary School recognises the essential and important contribution that technology plays in promoting children's learning and development, believe it and offers a fantastic range of positive activities and experiences. We do recognise however that this can bring risks. We take your child's online safety seriously and, as such, will take all reasonable precautions, including monitoring and filtering systems, to ensure that pupils are safe when they use our internet and systems. This includes: only allowing the pupils to access the internet when supervised; ensuring that they use Safe Search engines when find information on the internet; ensuring they use passwords to access resources and directing them to websites which have been chosen specifically for the tasjk and previously checked by the class teacher.

We recognise however that no technical system can replace online safety education and believe that children themselves have an important role to play in developing responsible behaviour. 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, discuss the content with them and submit it via ParentMail.

We understand that our children in Foundation Stage and KS1 are 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.

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.

We request that all parents support our approach to online safety by role modelling safe and positive online behaviour and by discussing online safety whenever children access technology at home. Parents can visit the school website's www.briary.kent.sch.uk under the **Parents** tab for more information about our approach to online safety. Full details of the school's online safety policy are available on the school website www.briary.kent.sch.uk/about/policies or on request. Parents/carers may also like to visit the following links for more information about keeping children safe online:

- www.thinkuknow.co.uk
- www.childnet.com
- www.nspcc.org.uk/onlinesafety
- www.saferinternet.org.uk
- www.internetmatters.org

Should you wish to discuss the matter further, please do not hesitate to contact myself as Designated Safeguarding Lead for Online Safety.

Yours sincerely,

Headteacher

Parent/Carers Acceptable Use Policy

1. I have read and discussed Briary Primary School 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 for Online Safety, Mrs Murrell, the Lead DSL, Mrs Symons or my child's teacher if I have any concerns about online safety.
9. I will visit the school website (www.briary.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.
12. I understand that my child needs a safe and appropriate place to access remote learning if school is closed in response to Covid-19. I will ensure my child's access to remote learning is appropriately supervised. When accessing on-line meetings (Teams), I will ensure they are in an appropriate location (e.g. not in bed) and that they are suitably dressed.

I have read, understood and agree to comply with the Briary Primary School Acceptable Use Policy.

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

Parents Name…………………………………………........

Staff Acceptable Use Policy

As a professional organisation with responsibility for safeguarding, it is important that 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 technology, they are asked to read and sign this Acceptable Use Policy.

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

1. I understand that Information Systems and IT 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. I will protect the devices in my care from unapproved access or theft.

4. I will respect system security and will not disclose any password or security information. I will use a 'strong' password to access school systems. 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. I will change my password when, and as, prompted by the School's system.

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 legislation (including GDPR).
   - 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 or accessed remotely.
   - Any data being removed from the school site (such as via email or on memory sticks or CDs) will be suitably protected. This may include data being 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 (link) and will always reflect parental consent.

7. I will not keep documents which contain school-related sensitive or personal information, including images, files, videos and emails, on any personal devices, such as laptops, digital cameras, and mobile phones. Where possible, I will use the School Sharepoint site to upload any work documents and files in a password protected environment or via VPN.

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 IT use, including using appropriate devices, safe use of social media and the supervision of pupils within the classroom and other working spaces.

11. I will immediately report any illegal, inappropriate or harmful material or incidents I become aware of, to the Designated Safeguarding Lead for Online Safety, Mrs Murrell.

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, I will report this to the Technician, Mr Jordan as soon as possible.

13. My electronic communications with current or past pupils, parents/carers and other professionals will 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 a school provided email address or telephone number, and not via my personal devices or communication channels, such as personal email, social networking or mobile phones unless specific and explicit permission has been sought and given by the headteacher.
    - Any pre-existing relationships or situations that may compromise this will be discussed with the Designated Safeguarding Lead for Online Safety, Mrs Murrell and/or headteacher.

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

15. I will not create, transmit, display, publish or forward any material online that is likely to harass, cause offence, inconvenience or needless anxiety to any other person, or anything which could bring my professional role, the school, the EKC Schools Trust or the County Council, into disrepute.

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

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

18. I understand that my use of the school information systems, including any devices provided by the school, including the 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.

19. I understand that the school may exercise its right to monitor the use of information systems, including internet access and the interception of emails, to monitor policy compliance. Where it believes unauthorised and/or inappropriate use, or unacceptable or inappropriate behaviour may be taking place, the school may invoke its disciplinary procedures. 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, understood and agreed to comply with Briary Primary School Staff Acceptable Use Policy

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

Letter for Staff

Please note this letter does NOT replace the Staff AUP

Dear member of staff name

At Briary Primary School, we recognise that staff can be vulnerable to online risks. Social media can blur the definitions of personal and working lives; it is important that all members of staff at Briary Primary School take precautions to protect themselves both professionally and personally online. We request that all members of staff:

- Are conscious of their own professional reputation and that of the school when 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.
  - Content shared online cannot be guaranteed to be "private" and could potentially be seen by unintended audiences. This could have consequences including civil, legal and disciplinary action being taken.

- Are aware that as professionals, we must ensure that the content we post online does not bring the school or our professional role into disrepute and does not undermine professional confidence in our abilities.
  - The teaching standards state that as professionals we should be achieving the highest possible standards in our conduct, act with honesty and integrity and forge positive professional relationships.

- All Staff be careful when publishing any information, personal contact details, video or images online.
  - 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.
  - Ensure that the privacy settings of the social media sites you use are set appropriately.
  - Consider if you would feel comfortable about a current or prospective employer, colleague, child in your care or their parent/carer, viewing or sharing your content. If the answer is no, consider if it should be posted online at all.

- Do not 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.
  - If you have a pre-existing relationship with a child or parent/carer or any other situation that may compromise this, speak to the Designated Safeguarding Lead for Online Safety, Mrs Murrell.

- Always use a work provided email address or phone number to contact children and parents – this is essential to protect yourself as well as the wider community.

- If you are concerned about a child's wellbeing or online behaviour, please speak to the Designated Safeguarding Lead for Online Safety, Mrs Murrell. If you are targeted online by a member of the community or are concerned about a colleague, then please speak to the headteacher and/or Chair of Governors.

  - If you are unhappy with the response you receive, or do not feel able to speak to the Designated Safeguarding Lead, headteacher or chair of governors then we request you follow our Whistleblowing procedure

- If you have any questions regarding online conduct expected of staff, please speak to the Designated Safeguarding Lead for Online Safety, Mrs Murrell and/or the Lead DSL, Mrs Symons.

Documents called “Cyberbullying: Supporting School Staff”, “Cyberbullying: advice for headteachers and school staff” and “Safer professional practise with technology” are available in the staffroom (or other locations for example school intranet) to help you consider how to protect yourself online.

Please photocopy them if you want or download the documents directly from:

- www.childnet.com/teachers-and-professionals/for-you-as-a-professional
- www.gov.uk/government/publications/preventing-and-tackling-bullying
- www.saferinternet.org.uk
- www.kscb.org.uk/guidance/online-safety

Additional advice and guidance for professionals is available locally through the Education Safeguarding Team or nationally through Professional Unions and/or the Professional Online Safety helpline www.saferinternet.org.uk/about/helpline

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 behaviour policy/code of conduct could lead to disciplinary action; it is crucial that all staff understand how to protect themselves online.

Please speak to your line manager, the Designated Safeguarding Lead Mrs Symons or myself if you have any queries or concerns regarding this.

Yours sincerely,

Headteacher

Additional regarding online participation on behalf the School, if applicable

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.

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, including visitors and volunteers, are fully aware of their professional responsibilities and read and sign this Acceptable Use Policy.

This is not an exhaustive list; 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.

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 for Online Safety, Mrs Murrell and/or the Lead DSL, Mrs Symons.

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, I will raise them with the Designated Safeguarding Lead for Online Safety, Mrs Murrell or the Lead DSL, Mrs Symons.

9. I will report any incidents of concern regarding children's online safety to the Designated Safeguarding Lead for Online Safety, Mrs Murrell 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, understood and agree to comply with the Briary Primary School Visitor /Volunteer Acceptable Use Policy.

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

Wi-Fi Acceptable Use Policy

For those using setting provided Wi-Fi. Settings may wish to use a paper or electronic AUP for guest access of Wi-Fi by members of the community. This template is provided for settings to adapt and use as appropriate.

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.

1. The school provides Wi-Fi for the school community and allows access for education use only.

2. I am 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.

3. The use of ICT devices falls under Briary Primary School's Acceptable Use Policy, online safety policy, behaviour policy and child protection policy which all pupils/staff/visitors and volunteers must agree to and comply with.

4. 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.

5. School owned information systems, including Wi-Fi, must be used lawfully; 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.

6. 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.

7. 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. I confirm that I knowingly assume such risk.

8. The school accepts no responsibility for any software downloaded and/or installed, email 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.

9. The school accepts no responsibility regarding the ability of equipment, owned by myself, to connect to the school's wireless service.

10. I will respect system security; I will not disclose any password or security information that is given to me. To prevent unauthorised access, I will not leave any information system unattended without first logging out or locking my login as appropriate.

11. I will not attempt to bypass any of the schools' security and filtering systems or download any unauthorised software or applications.

12. My use of 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.

13. 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.

14. I will report any online safety concerns, filtering breaches or receipt of inappropriate materials to the Designated Safeguarding Lead for Online Safety, Mrs Murrell as soon as possible.

15. If I have any queries or questions regarding safe behaviour online, I will discuss them with Designated Safeguarding Lead for Online Safety, Mrs Murrell or the Lead DSL, Mrs Symons.

16. I understand that my use of the school Wi-Fi may 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 may terminate or restrict usage. If the school suspects that the system may be being used for criminal purposes, the matter will be brought to the attention of the relevant law enforcement organisation.

I have read, understood and agree to comply with Briary Primary School Wi-Fi Acceptable Use Policy.

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

Official Social Networking Acceptable Use Policy for Staff

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 the Facebook and Twitter accounts provide 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 the school Designated Safeguarding Lead for Online Safety, Mrs Murrell and/or the Lead DSL, Mrs Symons. 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 taken for the sole purpose of inclusion on Facebook or Twitter 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 the 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 Facebook and Twitter account/site/page and I will use a strong password to secure the account. Personal social networking accounts or email addresses will not be used.
    - The school Designated Safeguarding Lead and/or headteacher will have full admin rights to the Facebook and Twitter site/page/group.

8. Where it believes unauthorised and/or inappropriate use of the Facebook or Twitter account 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.

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 and/or Designated Safeguarding Lead urgently.

11. I will ensure that the Facebook and Twitter accounts are 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 IT use, including using appropriate devices and the 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 the Designated Safeguarding Lead for Online Safety, Mrs Murrell or the headteacher.

I have read, understood and agree to comply with the Briary Primary School Social Networking Acceptable Use policy.

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

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