

Bratton Primary School



Acceptable Use Policy

2021-24

Bratton Primary School recognise the important contribution and value technology can play in promoting students' learning and development, however, there are potential risks involved. We have rigorous online safety policy and procedures in place and have taken positive steps to reduce this risk in school as we believe that the benefits to students from access to the Internet, in the form of information resources and opportunities for collaboration, exceed any disadvantages.

Allowing the use of mobile devices is a school decision, and should be subject to the following key principles:

- All individuals are protected from inappropriate material, bullying and harassment
- Users have access to resources to support learning and teaching
- Users should be given clear boundaries on responsible and professional use
- Access to network services is given to users who act in a considerate, appropriate and responsible manner.
- Users are responsible for their behaviour on school networks just as they are in any part of the school.
- Access is a privilege, not a right, and entails responsibility. We expect all users to use technology, both that belonging to the school or their own, responsibly and strictly according to the following conditions:

For the purposes of this document, technology means any device that provides a connection to the Internet or internal network.

1. A device loaned to you by the school for an education related purpose remains the property of Bratton Primary School
2. Only approved user devices may connect to the school network by prior agreement.
3. A device must remain in your possession, should only be used by you and should be securely stored when not in use.
4. Bratton Primary School policies regarding the appropriate use and sharing information apply to devices both school and privately owned. Use of any device must adhere to data protection, online safety and health and safety rules.
5. Devices may be used for education related purposes at the discretion and under the supervision of the teacher or responsible adult.
6. If used to create or store personal information including images and video of pupils, users must fully comply with high standards of data protection as set out in the Data Protection Act 1998.
7. A device connecting to the school network may be not be used with any device.
8. Visitors that come into school to provide training or assemblies etc must either use their own laptop, email the presentation beforehand or use a school computer using a guest login.
9. Insurance cover provides protection for school owned devices from the standard risks whilst the device is on site or in your home but excludes theft from a car or other establishment. Should the device be left unattended and is stolen, you will be responsible for its replacement.
10. Privately owned devices remain the responsibility of the owner and will not be covered under the school insurance policy.
11. All devices whether owned by the school or privately owned, may be subject to regular checks for compliance with school policies. Failure to comply or evidence of unacceptable use will result in sanctions or disciplinary action.

Bratton Primary School

Carpenter's Lane, Bratton, Westbury, Wiltshire BA13 4RL
Email: admin@bratton.wilts.sch.uk Telephone : 01380 830511



Parent/Carers Acceptable Use Policy 2021

- 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 school's 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 (Mrs Carole Hawke), my child's teacher or the Head Teacher if I have any concerns about online safety (e-Safety)
- I will visit the school website www.bratton.wilts.ch.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

Please complete this section and return to the school office.

I have read the Parent/Carer Acceptable Use Policy

Child's Name: Class:

Parent/Carers Name:

Parent/Carers Signature:..... Date:



Bratton Primary School

Carpenter's Lane, Bratton, Westbury, Wiltshire BA13 4RL
Email: admin@bratton.wilts.sch.uk Telephone : 01380 830511



Dear Parent/Carer

All pupils use computer facilities including Internet access as an essential part of learning, as required by the National Curriculum. Your child will have the opportunity to access a wide range of information and communication technology (ICT) resources. This includes access to:

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

Bratton Primary 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. We have a sophisticated filtering and monitoring system which is essential to keep children safe.

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 IT and Online Safety (e-Safety) policy are available on the school website www.bratton.wilts.sch.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.bratton.wilts.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/parents, www.nspcc.org.uk/onlinesafety, www.internetmatters.org www.saferinternet.org.uk and www.childnet.com for more information about keeping children safe online. It is expected that all parents/carers will sign and agree to the AUP.

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.

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,

Mrs Emma Williams
Headteacher

Bratton Primary School

Carpenter's Lane, Bratton, Westbury, Wiltshire BA13 4RL
Email: admin@bratton.wilts.sch.uk Telephone : 01380 830511



Dear

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 and governors 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 and governors 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 and governors 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 myself.

Documents called "Cyberbullying: Supporting School Staff", "Cyberbullying: advice for headteachers and school staff" and "Safer professional practise with technology" are available 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 and governors 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 and governors understand how to protect themselves online.

Yours sincerely,

Mrs Emma Williams
Headteacher

Staff and Governors Acceptable Use Policy



As a professional organisation with responsibility for children's safeguarding it is important that all staff and governors 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 and governors have a responsibility to use the school's computer system in a professional, lawful, and ethical manner. To ensure that members of staff and governors 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. 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 9 or more characters, does not contain a dictionary word and is only used on one system and is changed regularly).
5. I will seek advice or permission to install any purchased or downloaded software, including browser toolbars, or hardware without permission from the system manager or IT lead.
6. I will not use any external device with school laptops or pc's.
7. 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.
8. I will not keep or access professional documents which contain school-related sensitive or personal information (including images, files, videos, emails etc.) on any personal devices (such as laptops, digital cameras, mobile phones), unless they are suitably secured and encrypted. Where possible I will use Staff Share to upload any work documents and files in a password protected environment. I will protect the devices in my care from unapproved access or theft.
9. I recognise that storing 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 is not recommended and that school equipment must not be used for personal gain.
10. I will respect copyright and intellectual property rights.
11. I have read and understood the school IT and 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.
12. I will report all incidents of concern regarding children's online safety to the Online Safeguarding Lead as soon as possible. I will report any accidental access, receipt of inappropriate materials, filtering breaches or unsuitable websites to Online Safeguarding Lead (Mrs Carole Hawke).

13. 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 Oakford Technology as soon as possible.

14. My electronic communications with pupils, parents/carers and other professionals will only take place within clear and explicit professional boundaries and will be transparent and open to scrutiny at all times. All communication will take place via school approved communication channels e.g. via a school provided email address or telephone number and not via personal devices or communication channels e.g. personal email, social networking or mobile phones. Any pre-existing relationships or situations that may compromise this will be discussed with the Senior Leadership team and/or Head Teacher.

15. 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.

16. 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.

17. 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.

18. 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 Online Safeguarding Lead (Mrs Carole Hawke) or the Head Teacher.

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

The School may exercise its right to monitor the use of information systems, including Internet access and the interception of emails in order to monitor policy compliance. Where it believes unauthorised and/or inappropriate use of the schools information system or unacceptable or inappropriate behaviour may be taking place, the School will invoke its disciplinary procedure. If the school suspects that the school system may be being used for criminal purposes then the matter will be brought to the attention of the relevant law enforcement organisation.

Please complete this section and return to the school office.

I have read the Staff and Governors Acceptable Use Policy

Print Name:

Signature:..... Date:

Accepted by: Print name:



Visitor/Volunteer Acceptable Use Policy 2021

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 IT and 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 confidentiality, data protection and use of images and will abide with copyright and intellectual property rights, child protection legislation, privacy and data protection law and other relevant civil and criminal legislation.
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 Head Teacher.
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. When/if I come into school to provide training or assemblies etc I will either use my own laptop, email the presentation beforehand or use a school computer using a guest login.
9. 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 Online Safeguarding Lead or the Headteacher.
10. I will report any incidents of concern regarding children's online safety to the Safeguarding Lead as soon as possible.

Please complete this section and return to the school office.

I have read the Visitor/Volunteer Acceptable Use Policy

Print Name:

Signature:..... Date:



Social Networking Acceptable Use Policy 2021



(Parents/Carers/Volunteers of Bratton Primary School)

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 tools such as Facebook, Twitter, the school's website and blog are public and global communication tools and that any content posted on these may reflect on the school, its reputation and services. I will not use social media 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.

1. I will not disclose information, make commitments or engage in activities on behalf of the school without authorisation from the school Online Safeguarding Lead (Mrs Carole Hawke) or the Head teacher. The head teacher retains the right to remove or approve content posted on behalf of the school. Where it believes unauthorised and/or inappropriate use of Facebook, Twitter, the school's website and blog 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.
2. 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.
3. 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 Facebook, Twitter, the school's website and blog will not be forwarded to any other person or organisation.
4. I will promote online safety in the use of Facebook, Twitter, the school's website and blog and will help to develop a responsible attitude to safety online and to the content that is accessed or created.
5. 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.
6. I will report any accidental access or receipt of inappropriate materials or inappropriate comments to the Safeguarding Lead and/or head teacher immediately.
7. I will ensure that social media is moderated on a regular basis as agreed with the Safeguarding Lead and/or Headteacher.
8. 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 Headteacher.
9. If I have any queries or questions regarding safe and acceptable practise online I will raise them with the Safeguarding Lead or the Headteacher.

Please complete this section and return to the school office.

**I have and understood and agree to comply with the School Parent Association
Networking Acceptable Use Policy**

Print Name:

Signature:..... Date:

Accepted by: Print name:



Staff and Governors Social Networking Acceptable Use Policy



(Staff and Governors of Bratton Primary School)

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, the school's website and blog 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 this social media 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 Online Safeguarding Lead -Mrs Carole Hawke and/or the Head teacher. The head teacher retains the right to remove or approve content posted on behalf of the school.
3. I will ensure that any content posted abides by copyright and intellectual property rights, child protection legislation, privacy and data protection law and other relevant civil and criminal legislation.
4. I will follow the school's policy regarding confidentiality and data protection/use of images. This means I will ensure that the school has written permission from parents/carers before using images or videos which include any members of the school community. Any images of pupils will be taken on school equipment, by the school and in accordance with the school image policy. Images which include pupils will only be uploaded by the school. These will be for the sole purpose of inclusion on Facebook, Twitter, the school's website and blog 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, the school's website and blog 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 Online Safeguarding Lead/Head teacher prior to use.
6. Where it believes unauthorised and/or inappropriate use of Facebook, Twitter, the school's website or blog unacceptable or inappropriate behaviour may be taking place, the school will exercise the right to ask for the content to be deleted or deactivated.
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 Head teacher and/or Online Safeguarding Lead urgently.
9. I will ensure that Facebook, the school's website and blog site/page is moderated on a regular basis as agreed with the school Online Safeguarding Lead.
10. I have read and understood the school online safety (e-Safety) policy which covers the requirements for safe ICT use, including using appropriate devices and the safe use of social media. I have ensured that the site has been suitably risk assessed and this use has been agreed by the head teacher.
11. If I have any queries or questions regarding safe and acceptable practise online I will raise them with the Safeguarding Lead or the Head teacher.

I have and understood and agree to comply with the School Social Networking Acceptable Use Policy

Print Name:

Signature:..... Date:



Accepted by: Print name: