BLETCHINGLEY VILLAGE
PRIMARY SCHOOL

Aiming high • Working together • Achieving our best

Online Safety policy

Aims

- To **provide safeguards and raise awareness**, which will enable users to control their online experiences and feel confident and happy using technology online.
- To ensure all staff **adopt safe practices** in the use of the internet and in the teaching of internet use to children.
- To **educate** children to be responsible and informed internet users.
- To **inform and support** parents in keeping their children safe on the internet at home, on PCs or other internet-enabled devices, e.g. consoles, smartphones and tablets.

Online Safety is part of the school's safeguarding responsibilities. This policy relates to other policies including those for **behaviour, safeguarding, anti-bullying, data handling, mobile phones and the safe use of images.**

Using this policy

- The School's designated Online Safety Coordinator is Mrs Sarah Fletcher
- The school will have a designated Computing and Online Safety Governor. The Computing and Online Safety Governor is:
- Our e-safety Policy has been written by the school, building on best practice and government guidance. It has been agreed by senior management and approved by governors.
- The e-safety policy was revised by: Sarah Fletcher and Debbie Gregori
- It was approved by the Governors on:
- The e-safety policy and its implementation will be reviewed annually. The next review is due in November 2019
- The e-safety policy covers the use of all technology which can access the school network and the internet or which facilitates electronic communication from school to beyond the bounds of the school site. This includes but is not limited to workstations, laptops, mobile phones, tablets and hand held games consoles used on the school site.
- The e-safety policy recognises that there are differences between the use of technology as a private individual and as a member of staff / pupil.

Managing access and security

The school will provide managed internet access to its staff and pupils in order to help pupils to learn how to assess and manage risk, to gain the knowledge and understanding to keep themselves safe when using the internet and to bridge the gap between school IT systems and the more open systems outside school.

- The school will use a recognised internet service provider or regional broadband consortium.
- The school will ensure that all internet access has age appropriate filtering provided by a recognised filtering system which is regularly checked to ensure that it is working, effective and reasonable.
- The school will ensure that its networks have virus and anti-spam protection.
- Access to school networks will be controlled by personal passwords.
- Systems will be in place to ensure that internet use can be monitored and a log of any incidents will be kept to help to identify patterns of behaviour and to inform online safety policy.
- The security of school IT systems will be reviewed regularly.
- All staff that manage filtering systems or monitor IT use will be supervised by senior management and have clear procedures for reporting issues.
- The school will ensure that access to the internet via school equipment for anyone not employed by the school is filtered and monitored.

Internet Use

The school will provide an age-appropriate online safety curriculum, through our Computing scheme of work 'Fantastict', that teaches pupils how to stay safe, how to protect themselves from harm and how to take responsibility for their own and others' safety.

All communication between staff and pupils or families will take place using school equipment and/or school accounts.

As part of our Online Safety curriculum, pupils will be advised not to give out personal details or information which may identify them or their location**.**

E-mail

- Pupils, staff and Governors may only use approved e-mail accounts on the school IT systems.
- Staff to parent electronic communication must only take place via a school email address or agreed apps. Currently these are Study Bugs and marvellous Me.
- Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.
- The school will consider how e-mail from pupils to external bodies is presented and controlled.

Apps

- The preferred method of whole-school communication is currently the Study Bugs app, which also allows parents to inform the office about illness. Class communication form teachers is usually through marvellous Me. Both apps are free to download and support the school's 'Paper Free' philosophy.

Published content e.g. school web site

- The contact details will be the school address, email and telephone number. Staff or pupils' personal information, other than their name, will not be published.
- The head teacher or nominee will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing pupils' images and work

- Written permission will be obtained from parents or carers before photographs or names of pupils are published on the school web site or any school run social media as set out in Surrey Safeguarding Children Board Guidance on using images of children.
  http://www.surreycc.gov.uk/?a=168635
- The school will control access to social networking sites and consider how to educate pupils in their safe use. This control may not mean blocking every site; it may mean monitoring and educating students in their use.
- Use of video services such as Skype, Google Hangouts and Facetime will be monitored by staff. Pupils must ask permission from a member of staff before making or answering a video call.
- Staff and pupils should use ensure that their online activity, both in school and out, takes into account the feelings of others and is appropriate for their situation as a member of the school community.

Use of personal devices

- Personal equipment may be used by staff and/or pupils to access the school IT systems provided their use complies with the online safety policy, mobile phones policy and the relevant AUP.
- Staff must not store images of pupils or pupil personal data on personal devices.
- The school cannot be held responsible for the loss or damage of any personal devices used in school or for school business.

Protecting personal data

- The school has separate Data Protection and Confidentiality policies. They cover the use of biometrics in school, access to pupil and staff personal data on and off site, remote access to school systems.

Policy Decisions

Authorising access

- All staff (including teaching assistants, support staff, office staff, midday supervisors, premises managers, student teachers, work experience trainees, ICT technicians and governors) must read and sign the 'Staff AUP' before accessing the school IT systems.
- The school will maintain a current record of all staff and pupils who are granted access to school IT systems.
- At Key Stage 1, access to the internet will be by adult permission with supervised* access to specific, approved on-line materials.

- At Key Stage 2, access to the internet will be by adult permission with increasing levels of autonomy.
- People not employed by the school must read and sign a Visitor AUP before being given access to the internet via school equipment.
- Parents will be asked to sign and return a consent form to allow use of technology by their pupil.

*Not always in direct supervision of an adult.

Assessing risks

- The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor SCC can accept liability for the material accessed, or any consequences of internet access.

Handling Online Safety complaints

- Complaints of internet misuse will be dealt with according to the School Behaviour policy.
- Complaints of a child protection nature must be dealt with in accordance with school Child Protection procedures.
- Pupils and parents will be informed of consequences and sanctions for pupils misusing the internet and this will be in line with the schools' behaviour and online safety policy (see rules and sanctions Appendix).
- Complaints regarding misuse of data will be dealt with by the Data Protection Lead, Jo Vigar

Community use of the internet

- Members of the community and other organisations using the school internet connection will have signed a guest AUP so it is expected that their use will be in accordance with the school e-safety policy.

Communication of the Policy

To pupils

- Pupils need to agree to comply with the school 'SMART' online safety rules, in order to gain access to the school IT systems and to the internet.
- Pupils will be reminded about the contents of the school 'SMART' online safety rules as part of their e-safety education.

To staff

- All staff will be shown where to access the online safety policy and its importance explained.
- All staff must sign and agree to comply with the staff AUP in order to gain access to the school IT systems and to the internet
- All staff will receive online safety training (at an appropriate level) on an annual basis

To parents

- The school will ask all new parents to sign the parent /pupil agreement when they register their child with the school.

- Parents’ and carers’ attention will be drawn to the School Online Policy on the school web site.
- Parents will be offered online safety training across the year.

Appendix 1

BLETCHINGLEY VILLAGE
PRIMARY SCHOOL

Aiming high • Working together • Achieving our best

Staff
Acceptable Use Policy / ICT Code of Conduct
Bletchingley Village Primary School

ICT and the related technologies such as email, the internet and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to have read the online safety policy, sign this AUP and adhere to its contents and the contents of the online safety policy at all times. Any concerns or clarification should be discussed with Sarah Jowitt, Bletchingley Village Primary School's online safety coordinator.

- I appreciate that ICT includes a wide range of systems, including mobile phones, tablets, digital cameras, email, social networking and that ICT use may also include personal ICT devices when used for school business.

- I understand that it is a criminal offence to use a school ICT system for a purpose not permitted by its owner.

- I will only use the school's email / internet / intranet / Learning Platform and any related technologies for professional purposes, or for uses deemed 'reasonable' by the Head or Governing Body.

- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities.

- I understand that I am responsible for all activity carried out under my username.

- I will only use the approved, secure email system(s) for any school business.

- I will ensure that all electronic communications with parents, pupils and staff, including email, IM and social networking, are compatible with my professional role and that messages are clear and unambiguous.

- I will ensure that personal data (such as data held on SIMS or memory stick) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Head teacher or Governing Body.

- I will only take images of pupils and/or staff for professional purposes in line with school policy and these will be taken with a School resource (camera/tablet). I will not take any photos of children or staff off the school premises unless previously agreed by the Head teacher. I will not distribute images outside the school network/learning platform without the permission of the Head teacher.

- I will not install any hardware or software without the permission of Online Safety Coordinator or ICT Technician.

- I will not browse, download, upload or distribute any material that could be considered offensive, illegal, discriminatory or bring my professional role into disrepute.

- I will respect copyright and intellectual property rights.

- I understand that all my use of the internet and other related technologies can be monitored and logged and can be made available, on request, to my Line Manager or Head teacher.

- I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.

- I will support the school's online safety policy and help pupils to be safe and responsible in their use of ICT and related technologies. I will promote online safety with students in my care and will help them to develop a responsible attitude to system use, communications and publishing.

- I will report any incidents of concern regarding children's safety to the online safety Coordinator, the Designated Child Protection Officer or Head teacher.

- I understand that sanctions for disregarding any of the above will be in line with the school's disciplinary procedures and serious infringements may be referred to the police.

User Signature

I agree to follow this code of conduct and to support the safe use of ICT throughout the school.

Full Name……………………………………………………………………………………… (Printed)

Job title…………………………………………………………………………………………………

Signature……………………………………………… Date……………………

If there is anything in this AUP that you do not fully understand it is essential that you speak to one of the members of staff listed below before using the Bletchingley Village Primary School's ICT Network in order to ensure you use the ICT Network appropriately:

Sarah Jowitt	Online Safety Co-ordinator
Sarah Jowitt	Computing Coordinator
Stephanie Gibson/ Debbie Gregori	Senior Staff Member responsible for Behaviour Management
Ian Hunt	ICT Technican

Appendix 2

BLETCHINGLEY VILLAGE
PRIMARY SCHOOL

Aiming high • Working together • Achieving our best

Visitor Template
Acceptable Use Policy / ICT Code of Conduct
Bletchingley Village Primary School

- I understand that I have been given use of the school internet and/or school ICT systems in order to carry out a specific job for the school.
- I understand that it is a criminal offence to use a school ICT system for a purpose not permitted by its owner.
- I will only use the school's email / internet / intranet / Learning Platform and any related technologies for the purpose for which I have been given access.
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities.
- I will not install any hardware or software without the permission of Sarah Jowitt, Online Safety Coordinator or Ian Hunt, ICT technician.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory whilst using the school ICT systems.
- I understand that all my use of the internet and other related technologies can be monitored and logged and can be made available, on request, to the Head teacher or my employer.
- I will respect copyright and intellectual property rights.
- I understand that if I disregard any of the above then it will be reported to my employer and serious infringements may be referred to the police.

User Signature

I agree to follow this code of conduct and to support the safe use of ICT throughout the school.

Full Name……………………………………………………………………………… (Printed)

Company…………………………………………………………………………………………

Signature……………………………………………… Date……………………

If there is anything in this AUP that you do not fully understand it is essential that you speak to one of the members of staff listed below before using the Bletchingley Village Primary School's ICT Network in order to ensure you use the ICT Network appropriately:

Sarah Jowitt	Online Safety Co-ordinator
Sarah Jowitt	Computing Coordinator
Stephanie Gibson/ Debbie Gregori	Senior Staff Member responsible for Behaviour Management
Ian Hunt	ICT Technican

Appendix 3

BLETCHINGLEY VILLAGE
PRIMARY SCHOOL

Aiming high • Working together • Achieving our best

Bletchingley Village Primary School

Parent/Carer consent form and Online Safety Rules

All pupils use computer facilities, including internet access, as an essential part of learning, as required by the National Curriculum. Both pupils and their parents/carers are asked to sign agreements to show that the Online Safety Rules have been understood and agreed.

Parent / Carer name: ………………………………………………………….

Pupil name: ……..…………………………………………………………

As the parent or legal guardian of the above pupil, I have read and understood the attached school Online Safety rules and grant permission for my child to have access to use the internet, school email system, learning platform and other ICT facilities at school.

I know that my child has signed to say they will adhere to the school's online safety rules and that they have a copy of the school online rules in every classroom which are referred to constantly. We have discussed this document and my child agrees to follow the online safety rules and to support the safe and responsible use of ICT at Bletchingley Village Primary School.

I accept that ultimately the school cannot be held responsible for the nature and content of materials accessed through the internet and mobile technologies, but I understand that the school will take every reasonable precaution to keep pupils safe and to prevent pupils from accessing inappropriate materials. These steps include using an educationally filtered service, restricted access email, employing appropriate teaching practice and teaching online safety skills to pupils.

I understand that the school can check my child's computer files and the internet sites that they visit, and that if they have concerns about their online safety or e-behaviour they will contact me.

I understand the school is not liable for any damages arising from my child's use of the internet facilities.

I will support the school by promoting safe use of the internet and digital technology at home and will inform the school if I have any concerns over my child's online safety.

Parent/Guardian signature:

…………………………………………………………..Date…………………………………………….

Appendix 4

Bletchingley Village Primary School
Online Safety Rules KS1 and 2

At Bletchingley Village Primary School we follow the 'SMART' rules for staying safe online. Members of staff regularly refer to these and they are displayed in every learning area of our school.

Safe - Keep safe by being careful not to give out personal information when you're chatting or posting online. Personal information includes your email address, phone number and password.

Meeting - Meeting someone you have only been in touch with online can be dangerous. Only do so with your parents' or carers' permission and even then only when they can be present. Remember online friends are still strangers even if you have been talking to them for a long time.

Accepting - Accepting emails, IM messages, or opening files, pictures or texts from people you don't know or trust can lead to problems – they may contain viruses or nasty messages!

Reliable - Someone online might lie about who they are and information on the internet may not be true. Always check information with other websites, books or someone who knows. If you like chatting online it's best to only chat to your real world friends and family

Tell - Tell your parent, carer or a trusted adult if someone or something makes you feel uncomfortable or worried, or if you or someone you know is being bullied online.

Be smart on the internet
Childnet International
www.childnet.com
s
m
a
r
t
THINK U KNOW
KidSMART

SAFE Keep safe by being careful not to give out personal information – such as your full name, email address, phone number, home address, photos or school name – to people you are chatting with online.

MEETING Meeting someone you have only been in touch with online can be dangerous. Only do so with your parents' or carers' permission and even then only when they can be present.

ACCEPTING Accepting emails, IM messages, or opening files, pictures or texts from people you don't know or trust can lead to problems – they may contain viruses or nasty messages!

RELIABLE Information you find on the internet may not be true, or someone online may be lying about who they are.

TELL Tell your parent, carer or a trusted adult if someone or something makes you feel uncomfortable or worried, or if you or someone you know is being bullied online.

You can report online abuse to the police at www.thinkuknow.co.uk

www.kidsmart.org.uk

Visit Childnet's Kidsmart website to play interactive games and test your online safety knowledge. You can also share your favourite websites and online safety tips by Joining Hands with people all around the world.

Negative choices	Course of action	Possible negative consequences/sanctions	Recording
Level 1 Low level disruption could include: • Talking when asked not to • Distracting others • Not getting on with work • Going off task when using a device	1. Remind the child of the rule 2. Remind the child again of the rule and of the choices and consequences 3. Move the child within class	• Looks of disapproval/gesture • Removal of belongings • Moving seat • Sitting on own/single desk • Time Out/Special chair • Missing play to complete or re-do work to an acceptable standard	Class Log (no recording if online safety)
Level 2 *Serious misdemeanours* could include: • Lying • Answering back a member of staff • Defiance • General swearing aloud • Wilful damage • Persistent low level disruption • Searching, looking at or creating inappropriate content.	4. Send the child to another class 5. Send the child to Phase Leader.	• Missing play to complete or re-do work to an acceptable standard • Detention • Inform home • Meeting with parents/carers • Internal exclusion • No internet or device usage for a chosen period of time (days)	Central behaviour log Possible Individual Behaviour log Class teacher to record incident on Online Safety log
Level 3 • Persistent serious misdemeanours • Deliberately hurting someone • Dangerous or injurious behaviour • Bullying and racist incidents • Swearing at an adult • Continuous misuse of devices.	6. Send the child to Deputy Head Teacher	• Playground or classroom exclusion (kept off the playground) • Longer internal exclusion • Meeting with parents/carers • Letter of warning • No internet or device usage for a longer period of time (weeks)	Central behaviour log Behaviour log Behaviour plan EPC log Online Safety log
Level 4 • Extreme dangerous or injurious behaviour • Internal exclusions have been ineffective	7. Send child to Head Teacher	• Fixed-term exclusion • No device/ internet usage for the remainder of the year.	
Level 5 Fixed-term exclusions have been ineffective or there is a single incident which meets		• Permanent exclusion	