



Benington C of E Primary School

e-Safety Policy / Data Security Policy (including safe use of images)

Written	Reviewed	Next Review Date	Author	Adopted by Governors	Sub-Policies
Jan 2012	Dec 2019	Dec 2020	Anja Tyler		

E-Safety Policy & IT Acceptable Usage Agreement (AUA)

Rationale

As a Church School working with our local, national and international communities, IT in the 21st Century is seen as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, schools need to build in the use of these technologies in order to arm our young people with the skills to access life-long learning and employment.

Information and Communications Technology covers a wide range of resources including; web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of computing within our society as a whole. Currently the internet technologies children and young people are using both inside and outside of the classroom include:

- Websites
- Apps
- E-mail, Instant Messaging and chat rooms
- Social Media, including Facebook and Twitter
- Mobile/ Smart phones with text, video and/ or web functionality
- Other mobile devices including tablets and gaming devices
- Online Games
- Learning Platforms and Virtual Learning Environments
- Blogs and Wikis
- Podcasting
- Video sharing
- Downloading
- On demand TV and video, movies and radio / Smart TVs

Whilst exciting and beneficial both in and out of the context of education, much IT, particularly web-based resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these Internet technologies and that some have minimum age requirements (13 years in most cases).

At Benington Primary School, we understand the responsibility to educate our pupils on e-safety issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

Both this policy and the Acceptable Use Agreements (for all staff, governors, visitors and pupils) are inclusive of both fixed and mobile internet; technologies provided by the school (such as PCs, laptops, I pads webcams, whiteboards, digital video equipment, etc); and technologies owned by pupils and staff, but brought onto school premises (such as laptops, mobile phones, smart phones, and portable media players, etc).

Roles and Responsibilities

As e-safety is an important aspect of strategic leadership within the school the Governing Body have ultimate responsibility to ensure that the policy and practices are embedded and monitored. This responsibility is delegated to the Head. Any extra permission given by the Head must be recorded (e.g. memos, minutes from meetings) in order to be valid.

The named person (Safeguarding Officer) and Computing Co-ordinator have the responsibility of ensuring this policy is upheld by all members of the school community and that they have been made aware of the implication this has. It is the role of these members of staff to keep abreast of current issues and guidance through organisations such as the LA, Becta, CEOP (Child Exploitation and Online Protection), Childnet and Local Authority Safeguarding Children Board.

This policy, supported by the school's acceptable use agreements for staff, governors, visitors and pupils (appendices), is to protect the interests and safety of the whole school community. It is linked to the following mandatory school policies: child protection, health and safety, home-school agreements, safeguarding policy and behaviour/pupil discipline (including the anti-bullying) policy.

E-safety skills development for staff

- Our staff receive regular information and training on e-safety issues in the form of full staff meetings and memos.
- New staff receive information on the school's acceptable use policy as part of their induction through their staff handbooks.
- All staff have been made aware of individual responsibilities relating to the safeguarding of children within the context of e-safety and know what to do in the event of misuse of technology by any member of the school community.
- All staff are encouraged to incorporate e-safety activities and awareness within their curriculum areas.

Communicating the school e-safety messages

- E-safety rules will be posted in all networked rooms and discussed with the pupils at the start of each year and through each scheme of work.
- Pupils will be informed that network and Internet use will be monitored.
- E-safety posters will be prominently displayed in all classrooms.
- Visitors to school who will be working with pupils will be made aware, upon signing in, of our approach to e-safety by way of an information sheet.

E-Safety in the Curriculum

IT and online resources are increasingly used across the curriculum. We believe it is essential for e-safety guidance to be given to the pupils on a regular and meaningful basis, at least once a term, along with addressing issues as they arise. E-safety is embedded within our curriculum and we continually look for new opportunities to promote E-safety. We regularly monitor and assess our pupils' understanding of e-safety.

- The school provides opportunities within a range of curriculum areas and discrete computing lessons to teach about e-safety (in accordance with the medium term planning and the Herts scheme of work.)
- Educating pupils on the dangers of technologies that maybe encountered outside school may also be done informally when opportunities arise.
- Pupils are aware of the relevant legislation when using the internet such as data protection and intellectual property which may limit what they want to do but also serves to protect them.
- Pupils are taught about copyright and respecting other people's information, images, etc through discussion, modelling and activities.
- Pupils are aware of the impact of online bullying and know how to seek help if they are affected by these issues. Pupils are also aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent/ carer, teacher/ trusted staff member, or an organisation such as Childline/ CEOP report abuse button.
- Pupils are taught to critically evaluate materials and learn good searching skills through cross curricular teacher models, discussions and via the computing curriculum.

Data Security

- The school gives relevant staff access to its Management Information System, with a unique username and password
- It is the responsibility of everyone to keep passwords secure
- Staff are aware of their responsibility when accessing school data
- Staff have been issued with the relevant guidance documents and the Policy for ICT Acceptable Use
- Staff keep all school related data secure. This includes all personal, sensitive, confidential or classified data
- Staff should avoid leaving any portable or mobile ICT equipment or removable storage media in unattended vehicles. Where this is not possible, keep it locked out of sight
- Staff should always carry portable and mobile ICT equipment or removable media as hand luggage, and keep it under your control at all times
- It is the responsibility of individual staff to ensure the security of any personal or sensitive information contained in documents faxed, copied, scanned or printed. This is particularly important when shared mopiers (multi-function print, fax, scan and copiers) are used
- Anyone sending a confidential or sensitive fax should notify the recipient before it is sent

The accessing and appropriate use of school data is something that the school takes very seriously. Staff are aware of their responsibility when accessing school data. Level of access is determined by the Head Teacher. Data can only be accessed and used on school computers or laptops. Staff are aware that when using personal devices for accessing any school/pupil data, all data must be password protected.

Password Security

Password security is essential for staff, particularly as they are able to access and use pupil data. Staff have access to this through Administrator Rights on the HGFL network. The pupils from Year R upwards have individual logins and storage folders on the server. Staff and pupils are regularly reminded of the need for password security.

Managing the Internet

The internet is an open communication medium, available to all, at all times. Anyone can view information, send messages, discuss ideas and publish material which makes it both an invaluable resource for education, business and social interaction, as well as a potential risk to young and vulnerable people. Whenever any inappropriate use is detected it will be followed up.

- All staff must read and agree to the 'Acceptable IT Use Agreement' before using any school IT resource.
- At Key Stage 1, access to the Internet will be by adult demonstration with occasional directly supervised access to specific, approved on-line materials.
- Staff will preview any recommended sites before use.
- Raw image searches are discouraged when working with pupils.
- If Internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher. It is advised that parents recheck these sites and supervise this work. Parents will be advised to supervise any further research.
- All users must observe software copyright at all times. It is illegal to copy or distribute school software or illegal software from other sources.
- All users must observe copyright of materials from electronic resources.

Infrastructure

- School internet access is controlled through the LA's web filtering service.
- Our school also employs some additional web filtering.
- Staff and pupils are aware that school based email and internet activity can be monitored and explored further if required.
- If staff or pupils discover an unsuitable site, the screen must be switched off/ closed and the incident reported immediately to the class teacher who must inform an e-safety co-ordinator.
- It is the responsibility of the school, by delegation to the technical support; to ensure that Anti-virus protection (Sophos) is installed and kept up-to-date on all school machines.
- If pupils wish to bring in work on removable media it must be given to the teacher for a safety check first.
- Pupils and staff are not permitted to download programs or files on school based technologies without seeking prior permission from the Computing co-ordinator.
- If there are any issues related to viruses or anti-virus software, the IT Technician should be informed through the 'Computer Problems' book.

Managing other Web 2 technologies

Web 2, including social networking sites, if used responsibly both outside and within an educational context can provide easy to use, creative, collaborative and free facilities. However it is important to recognise that there are issues regarding the appropriateness of some content, contact, culture and commercialism. To this end, we encourage our pupils to think carefully about the way that information can be added and removed by all users, including themselves, from these sites.

- The school endeavours to deny access to unmonitored social networking sites such as Facebook to pupils within school.
- There should be no communication between staff and pupils through social networking sites such as Facebook.
- All pupils are advised to be cautious about the information given by others on sites, for example users not being who they say they are.
- Pupils are taught to avoid placing images of themselves (or details within images that could give background details) on such sites and to consider the appropriateness of any images they post due to the difficulty of removing an image once online.

- Pupils are always reminded to avoid giving out personal details on such sites which may identify them or where they are (full name, address, mobile/ home phone numbers, school details, IM/ email address, specific hobbies/ interests).
- Our pupils are advised to set and maintain profiles on such sites to maximum privacy and deny access to unknown individuals.
- Pupils are encouraged to be wary about publishing specific and detailed private thoughts online.
- Our pupils are asked to report any incidents of bullying to the school.

Mobile technologies

Many emerging technologies offer new opportunities for teaching and learning including a move towards personalised learning and 1:1 device ownership for children and young people. They often provide a collaborative, well-known device with possible internet access and thus open up risk and misuse associated with communication and internet use. Emerging technologies will be examined for educational benefit and the risk assessed before use in school is allowed. Our school chooses to manage the use of these devices in the following ways so that users exploit them appropriately.

Personal Mobile devices (including phones)

- The school allows staff to bring in personal mobile phones and devices for their own use. Under no circumstances does the school allow a member of staff to contact a pupil or parent/carer using their personal device, unless they use block caller id.
- Staff will be made aware of the potential dangers of giving out their personal number, and to use block caller id when appropriate.
- Pupils are not allowed to bring personal mobile devices/phones or smart watches to school unless this is for educational purposes set by the teacher (even then, strict monitoring and controlled usage will only be permitted).
- The school is not responsible for the loss, damage or theft of any personal mobile device.
- The sending of inappropriate text messages between any members of the school community is not allowed.
- Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.

Managing email

The use of email within most schools is an essential means of communication for both staff and pupils. Educationally, email can offer significant benefits including; direct written contact between schools on different projects, be they staff based or pupil based, within school or internationally. We recognise that pupils need to understand how to style an email in relation to their age and good 'etiquette'. Pupils must have experienced sending and receiving emails by the end of KS2.

- The school gives all staff their own email account to use for all school business. This is to minimise the risk of receiving unsolicited or malicious emails and avoids the risk of personal profile information being revealed.
- Staff sending e-mails to external organisations, parents or pupils are advised to cc. the Headteacher or designated line manager.
- It is the responsibility of each account holder to keep the password secure. This should be the account that is used for all school business.
- Under no circumstances should staff contact pupils, parents or conduct any school business using personal email addresses, unless deemed appropriate.

- E-mail sent to an external organisation should be written carefully before sending, in the same way as a letter written on school headed paper.
- Pupils may only use school approved accounts on the school system and only under direct teacher supervision for educational purposes.
- All e-mail users are expected to adhere to the generally accepted rules of network etiquette particularly in relation to the use of appropriate language and not revealing any personal details about themselves or others in e-mail communication, or arranging to meet anyone without specific permission, virus checking attachments.
- Pupils must immediately tell a teacher/ trusted adult if they receive an offensive e-mail.
- Staff must inform the computing co-ordinator if they receive an offensive e-mail.
- Pupils are introduced to email as part of the computing scheme of work at Year 5 & 6.

Safe Use of Images

Taking of Images and Film

Digital images are easy to capture, reproduce and publish and, therefore, misused. We must remember that it is not always appropriate to take or store images of any member of the school community or public, without first seeking consent and considering the appropriateness.

- With the written consent of parents (on behalf of pupils) and staff, the school permits the appropriate taking of images by staff and pupils with school equipment.
- Staff are not permitted to use personal digital equipment, such as mobile phones and cameras, to record images of pupils, this includes when on school trips unless for school use. Once photos are downloaded all pictures will be deleted from the device forthwith.
- Pupils are not permitted to use personal digital equipment, including mobile phones and cameras, to record images of others, this includes when on school trips. With the consent of the class teacher, pupils are permitted to take digital cameras from school to record images and can download these images on the school network.

Publishing pupil's images and work

On a child's entry to the school, all parents/carers will be asked to give permission to use their child's work/photos in the following ways:

- on the school web site and or FOBS Facebook page.
- in the school prospectus and other printed publications that the school may produce for promotional purposes
- recorded/ transmitted on a video or webcam
- in display material that may be used in the school's communal areas
- in display material that may be used in external areas, i.e. exhibition promoting the school
- general media appearances, e.g. local/ national media/ press releases sent to the press highlighting an activity (sent using traditional methods or electronically)

This consent form is considered valid for the entire period that the child attends this school unless there is a change in the child's circumstances where consent could be an issue, e.g. divorce of parents, custody issues, etc.

Parents/ carers may withdraw permission, in writing, at any time. Consent has to be given by both parents in order for it to be deemed valid.

Pupils' full names will not be published alongside their image and vice versa. E-mail and postal addresses of pupils will not be published.

Before posting pupils' work on the Internet, a check needs to be made to ensure that permission has been given for work to be displayed.

Storage of Images

Images/ films of children are stored on the school's network.

- Pupils and staff are not permitted to use personal portable media for storage of images (e.g., USB sticks) without the express permission of the Head Teacher
- Rights of access to this material are restricted to the teaching staff and pupils within the confines of the school network/ Learning Platform.
- Teaching Staff have the responsibility of deleting the images when they are no longer required, or when the pupil has left the school.

Misuse and Infringements

Complaints

- Complaints relating to e-safety should be made to the computing co-ordinator or Head Teacher.
- All incidents will be logged and followed up.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures and must be reported to the Named person (Safeguarding Officer).
- Pupils and parents will be informed of the complaints procedure.

Inappropriate material (see IT Acceptable Use Agreement)

- All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the e-safety co-ordinators.
- Deliberate access to inappropriate materials by any user will lead to the incident being logged by the computing co-ordinator, depending on the seriousness of the offence; investigation by the Head Teacher/ LA, immediate suspension, possibly leading to dismissal and involvement of police for very serious offences.
- Users are made aware of sanctions relating to the misuse or misconduct.

Breaches

A breach or suspected breach of policy by a school employee, contractor or pupil may result in the temporary or permanent withdrawal of school IT hardware, software or services from the offending individual.

For staff any policy breach is grounds for disciplinary action in accordance with the school Disciplinary Procedure or, for Support Staff, in their Probationary Period as stated.

Policy breaches may also lead to criminal or civil proceedings.

The Information Commissioner's powers to issue monetary penalties came into force on 6 April 2010, allowing the Information Commissioner's office to serve notices requiring organisations to pay up to £500,000 for serious breaches of the Data Protection Act.

The data protection powers of the Information Commissioner's Office are to:

- Conduct assessments to check organisations are complying with the Act;
- Serve information notices requiring organisations to provide the Information Commissioner's Office with specified information within a certain time period;

- Serve enforcement notices and 'stop now' orders where there has been a breach of the Act, requiring organisations to take (or refrain from taking) specified steps in order to ensure they comply with the law;
- Prosecute those who commit criminal offences under the Act;
- Conduct audits to assess whether organisations' processing of personal data follows good practice,
- Report to Parliament on data protection issues of concern

For pupils, reference will be made to the school's behaviour policy.

Incident Reporting

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of IT must be immediately reported to the school's relevant responsible person. Additionally, all security breaches, lost/stolen equipment or data (including remote access SecureID tokens and PINs), virus notifications, unsolicited emails, misuse or unauthorised use of IT and all other policy non-compliance must be reported to the relevant responsible person. The relevant responsible individuals in the school are as follows: Mr Bailes; Mrs Stevens; Miss Webb-Ingall.

Please refer to the relevant section on Incident Reporting, eSafety Incident Log & Infringements.

Equal Opportunities

Pupils with additional needs

The school endeavours to create a consistent message with parents for all pupils and this in turn should aid establishment and future development of the schools' e-safety rules.

However, staff are aware that some pupils may require additional teaching including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of e-safety issues.

Where a pupil has poor social understanding, careful consideration is given to group interactions when raising awareness of e-safety. Internet activities are planned and well managed for these children and young people.

Parental Involvement

We believe that it is essential for parents/ carers to be fully involved with promoting e-safety both in and outside of school. We regularly consult and discuss e-safety with parents/ carers and seek to promote a wide understanding of the benefits related to IT and associated risks.

- Parents/ carers are asked to read through and sign acceptable use agreements on behalf of their child on admission to school.
- Parents/ carers are required to make a decision as to whether they consent to images of their child being taken/ used in the public domain (e.g., on school website)
- The school disseminates information to parents relating to e-safety where appropriate in the form of;
 - Information sessions
 - Posters
 - Learning Platform postings/links to further information
 - Newsletter items

- Parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupil.
- Parents/carers are expected to reinforce the guidance from school when using technologies at home. The school will not be responsible for communications between pupils' outside school through social networking sites.

IT Acceptable Use Agreement (AUA)

POLICY STATEMENT

The Governing Body recognises the use of IT as an important resource for teaching, learning and personal development. It actively encourages staff to take full advantage of the potential for IT to enhance development in all areas of the curriculum and school administration. It is also recognised by the Governing Body that along with these benefits there are also responsibilities, especially for ensuring that children are protected from contact with inappropriate materials.

In addition to their normal access to the school's IT systems for work-related purposes, the Governing Body permits staff limited reasonable personal use of IT equipment and e-mail and internet facilities during their own time subject to such use:

1. *not depriving pupils of the use of the equipment
and/or*
2. *not interfering with the proper performance of the staff member's duties*

Whilst the school's IT systems may be used for both work-related and for personal reasons the Governing Body expects use of this equipment for any purpose to be appropriate, courteous and consistent with the expectations of the Governing Body at all times and must never compromise the high standards of Safeguarding expected by all members of the staff.

The use of computer equipment, including laptop computers, which is on loan to staff by the school for their personal use at home is covered under this policy. Staff who have equipment on loan are responsible for its safekeeping and for ensuring that it is used in compliance with this policy.

GUIDANCE ON THE USE OF SCHOOL IT FACILITIES

Whilst it is not possible to cover all eventualities, the following information is published as guidance for staff on the expectations of the Governing Body. Any non-conformance to this policy or operation outside statutory legal compliance may be grounds for disciplinary action being taken up to and including disciplinary action

Further guidance on the responsible use of IT facilities are contained in the Council document "*Internet Access Policy for Schools*".

E-mail and Internet usage

The following uses of the school's IT system are prohibited and may in certain circumstances amount to gross misconduct and could result in dismissal:

1. *to gain access to, and/or for the publication and distribution of inappropriate sexual material, including text and/or images, or other material that would tend to deprave or corrupt those*

likely to read or see it

2. *to gain access to, and/or for the publication and distribution of material promoting racial hatred*
3. *for the purpose of bullying or harassment, or for or in connection with discrimination or denigration on the grounds of gender, race, disability or sexual orientation*
4. *for the publication and/or distribution of libellous statements or material which defames or degrades others*
5. *for the publication and distribution of personal data without either consent or justification*
6. *where the content of the e-mail correspondence is unlawful or in pursuance of an unlawful activity, including unlawful discrimination*
7. *to participate in on-line gambling*
8. *where the use infringes copyright law*
9. *to gain unauthorised access to internal or external computer systems (commonly known as hacking)*
10. *to enable or assist others to breach the Governors' expectations as set out in this policy*

Additionally, the following uses of school IT facilities are not permitted and could lead to disciplinary action being taken:

1. *for participation in "chain" e-mail correspondence*
2. *in pursuance of personal business or financial interests, or political activities (excluding the legitimate activities of recognised trade union representatives)*
3. *to access IT facilities using another person's password, or to post anonymous messages or forge e-mail messages using another person's identity.*

Use of School IT Equipment

Users of school IT equipment:

1. *must not share and must treat as confidential any passwords provided to allow access to IT equipment and/or beyond firewall protection boundaries*
2. *must report any known breach of password confidentiality to the Headteacher or nominated IT Co-ordinator as soon as possible*
3. *must report known breaches of this policy, including any inappropriate images or other material which may be discovered on the school's IT systems*
4. *must not install software on the school's IT systems, including freeware and shareware, unless authorised by the school's IT Co-ordinator*

5. *must comply with any IT security procedures governing the use of systems in the school, including anti-virus measures*

Regulation of Investigatory Powers Act 2000

Ancillary to their provision IT facilities the Governing Body asserts the employer's right to monitor and inspect the use by staff of any computer or telephonic communications systems where there are grounds for suspecting that such facilities are being, or may have been, misused.

Social Media, including Facebook and Twitter

Facebook, Twitter and other forms of social media are increasingly becoming an important part of our daily lives. Staff, governors, pupils, parents and carers are regularly provided with information on how to use social media responsibly and what to do if they are aware of inappropriate use by others.

Acceptable Use Agreement: Staff and Governors

Acceptable Use Agreement / Code of Conduct

ICT (including data) and the related technologies such as e-mail, 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 technology. All staff are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with Mrs Tyler or Mrs Swann.

- I will only use the school's email / Internet / Intranet / Learning Platform and any related technologies for professional purposes or for uses deemed acceptable by the Head or Governing Body
- I will comply with the IT system security and not disclose any passwords provided to me by the school or other related authorities
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role
- I will not give out my own personal details, such as mobile phone number, personal e-mail address, personal Twitter account, or any other social media link, to pupils
- I will only use the approved, secure e-mail system(s) for any school business
- I will ensure that personal data (such as data held on MIS software) 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 or Governing Body. Personal or sensitive data taken off site must be encrypted, eg on a password secured laptop or memory stick
- I will not install any hardware or software without permission of computing co-ordinator
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory
- Images of pupils and/ or staff will only be taken, stored and used for professional purposes in line with school policy and with written consent of the parent, carer or staff member
- Images will not be distributed outside the school network without the permission of the parent/ carer, member of staff or Headteacher
- I will support the school approach to online safety and not upload or add any images, video, sounds or text linked to or associated with the school or its community'
- 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 Headteacher
- I will respect copyright and intellectual property rights
- I will ensure that my online activity, both in school and outside school, will not bring the school, my professional reputation, or that of others, into disrepute
- I will support and promote the school's e-Safety and Data Security policies and help pupils to be safe and responsible in their use of related technologies
- I understand this forms part of the terms and conditions set out in my contract of employment

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

Signature Date

Full Name(printed)

Job title

Smile and Stay Safe Poster

eSafety guidelines to be displayed throughout the school



Staying safe means keeping your personal details private, such as full name, phone number, home address, photos or school. Never reply to ASL (age, sex, location)

Meeting up with someone you have met online can be dangerous. Only meet up if you have first told your parent or carer and they can be with you

Information online can be untrue, biased or just inaccurate. Someone online may not be telling the truth about who they are - they may not be a 'friend'

Let a parent, carer, teacher or trusted adult know if you ever feel worried, uncomfortable or frightened about something online or someone you have met or who has contacted you online

Emails, downloads, IM messages, photos and anything from someone you do not know or trust may contain a virus or unpleasant message. So do not open or reply

Acceptable Use Agreement / eSafety Rules

- I will only use technologies in school for school purposes; these are laptops; Ipads; computers; smart technologies etc.
- I will only use my school e-mail address when e-mailing
- I will only open e-mail attachments from people I know, or who my teacher has approved
- I will not tell other people my passwords
- I will only open/delete my own files
- I will make sure that all computing contact with other children and adults is responsible, polite and sensible
- I will not look for, save or send anything that could be unpleasant or nasty. If I accidentally find anything like this I will tell my teacher **immediately**
- I will not give out my own/others details such as name, phone number or home address. I will not arrange to meet someone or send my image unless this is part of a school project approved by my teacher and a responsible adult comes with me
- I will be responsible for my behaviour when using any technology because I know that these rules are to keep me safe
- I will support the school approach to online safety and not upload or add any images, video, sounds or text that could upset any member of the school community
- I know that my use of any technology can be checked and my parent/carer contacted if a member of school staff is concerned about my safety
- I will not sign up for any online service unless this is an agreed part of a school project approved by my teacher
- I will not bring a Smart Watch to school because I am not allowed to wear one during the school day
- I will not sign up to online services until I am old enough

Benington C of E Primary School



Walkern Road, Benington, Hertfordshire SG2 7LP.
Telephone 01438 869 254
e-mail: admin@benington.herts.sch.uk www.benington.herts.sch.uk

Dear Parent/ Carer

Computing including the internet, e-mail and mobile technologies has become an important part of learning in our school. We expect all children to be safe and responsible when using any technology.

Please read and discuss these eSafety rules with your child and return the slip at the bottom of this page. If you have any concerns or would like some explanation please contact Mr Bailes.

Please take care to ensure that appropriate systems are in place at home to protect and support your child/ren. As part of this we have enclosed a family agreement that you might like to use at home as part of your home-school partnership.

✂

Parent/ carer signature

We have discussed this document with
.....(.....) and we agree to follow the
eSafety rules and to support the safe use of computing at Benington C of E Primary
School.

Parent/ Carer Signature

Class Date