Bampton CE Primary School and Nursery

Learning together with Respect, Friendship and Perseverance

School Vision Statement

We endeavour to enable individuals in our school community to learn together, grow in respect, tolerance and understanding of the world in which we live, embrace Christian values and reach our full potential.

Title of Policy	**E-safety policy and ICT acceptable user agreement**
Date Adopted by the Governing Body	**January 2019**
Review Date	**January 2021**
Signed by the Chair of Governors	

Bampton CE Primary School E-Safety Policy and ICT Acceptable Usage Agreement (AUA)

This policy applies to all members of the school community (including staff, students / pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of school / academy ICT systems, both in and out of the school.

The Education and Inspections Act 2006 empowers Head Teachers to such extent as is reasonable, to regulate the behaviour of students / pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other e-safety incidents covered by this policy, which may take place outside of the school / academy, but is linked to membership of the school / academy.

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate e-safety behaviour that take place out of school.

At Bampton CE 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, webcams, whiteboards, digital video equipment, etc); and technologies owned by staff, but brought onto school premises (such as laptops, mobile phones, camera phones, and portable media players, etc).

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 and anti-bullying policy.

Roles and Responsibilities

Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy.

The **Head Teacher** has a duty of care for ensuring the safety (including e-safety) of members of the school community and is responsible for ensuring that the ICT coordinator and other staff receive suitable training to enable them to carry out their e-safety roles.

The **Head Teacher** is the designated e-safety coordinator and therefore:

• takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / documents

• ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.

• provides training and advice for staff

• liaises with the Local Authority

• liaises with school technical staff and ICT coordinator

• receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments.

Teaching Staff and Support Staff are responsible for ensuring that:

• they have an up to date awareness of e-safety matters and of the current school e-safety policy and practices

• they have read, understood and signed the E safety Policy and Staff Acceptable Use Agreement

• they report any suspected misuse or problem to the Head Teacher for investigation / action / sanction

• all digital communications with students / pupils / parents / carers should be on a professional level and only carried out using official school systems

• e-safety issues are embedded in all aspects of the curriculum and other activities

• students / pupils understand and follow the e-safety and acceptable use policies

• students / pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations

• they monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities (where allowed) and implement current policies with regard to these devices

• in lessons where internet use is pre-planned pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

The Headteacher is the Child Protection Designated Officer and therefore should be trained in e-safety issues and be aware of the potential for serious child protection / safeguarding issues to arise from:

• sharing of personal data

• access to illegal / inappropriate materials

• inappropriate on-line contact with adults / strangers

• potential or actual incidents of grooming

• cyber-bullying

Students / pupils:

• are responsible for using the school digital technology systems in accordance with the Pupil Acceptable Use Policy

• have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations

• need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so

• will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking / use of images and on cyber-bullying.

• should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school.

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website and information about national / local e-safety campaigns / literature. Parents and carers will be encouraged to support the school in promoting good e-safety practice and to follow guidelines on the appropriate use of:

• digital and video images taken at school events

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.
- E-safety activities and awareness are reflected in the curriculum plans.

Communicating the school e-safety messages

- E-safety rules will be posted near computer stations and in the computer suite. These are and discussed with the pupils at the start of each year and reviewed when necessary.
- Pupils will be informed that network and Internet use will be monitored.
- E-safety posters will be prominently displayed, especially in the ICT suite.
- Internet Safety focus days for children and parents/carers
- E-safety events for parents/carers

E-Safety in the Curriculum

ICT 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. 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 ICT lessons to teach about e-safety (in accordance with the medium term planning.)
- 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 ICT curriculum.

Password Security

Password security is essential for staff, particularly as they are able to access and use pupil data.
Pupils in Foundation Stage and KS1 use group or class passwords. The pupils from Year 3 upwards have individual logins and storage folders on the server. Staff and pupils are regularly reminded of the need for password security and a password strength policy is in place to maximise security."

Creating a strong password

To create a stronger and more complex password, use passwords that are at least eight characters long, and that include at least one character from the four groups listed below.

1. Upper-case characters (A through Z)
2. Lower-case characters (a through z)
3. Numerals (0 through 9)
4. Non-alphabetic characters (for instance: ! $ # or %)

The password should not include your account name, your name or any dictionary word.
Passwords should be changed every 90 days and none of the last six passwords used should be re-used.

Data Security

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 they must not use their personal devices for accessing any school/pupil data.

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 ICT Use Agreement' before using any school ICT 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 web filtering service.
- 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 the Head Teacher.
- It is the responsibility of the school, by delegation to the technical support; to ensure that Anti-virus protection 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 Head Teacher.
- If there are any issues related to viruses or anti-virus software, the ICT technician should be informed through the 'Computer Problems' book held in the staff room.

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.
- Pupils are not allowed to bring personal mobile devices/phones to school.
- The school is not responsible for the loss, damage or theft of any personal mobile device.
- The sending of inappropriate text messages between any member 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 'netiquette' and have experienced sending and receiving emails.

- The school gives all staff and Governors 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.
- 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
- In support of staff maintaining a healthy work life balance there is no expectation that staff will read and respond to emails outside of reasonable working hours
- 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.
- The KS2 pupils have their own individual school issued accounts**,** all other children use a class/ group email address.
- 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 member of staff/trusted adult if they receive an offensive e-mail.
- Staff must inform the Head Teacher if they receive an offensive e-mail.
- Pupils are introduced to email as part of the ICT Scheme of Work in KS2.

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 to record images of pupils, this includes when on school trips. Staff may use a camera or video recorder to record images in line with this policy but must only download the images onto a school computer. Images must be downloaded immediately and cannot be stored on the device.
- 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

- 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
- USB sticks used by staff to store images and/or data must be password protected
- Rights of access to this material are restricted to the teaching staff and pupils within the confines of the school network.
- 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 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.

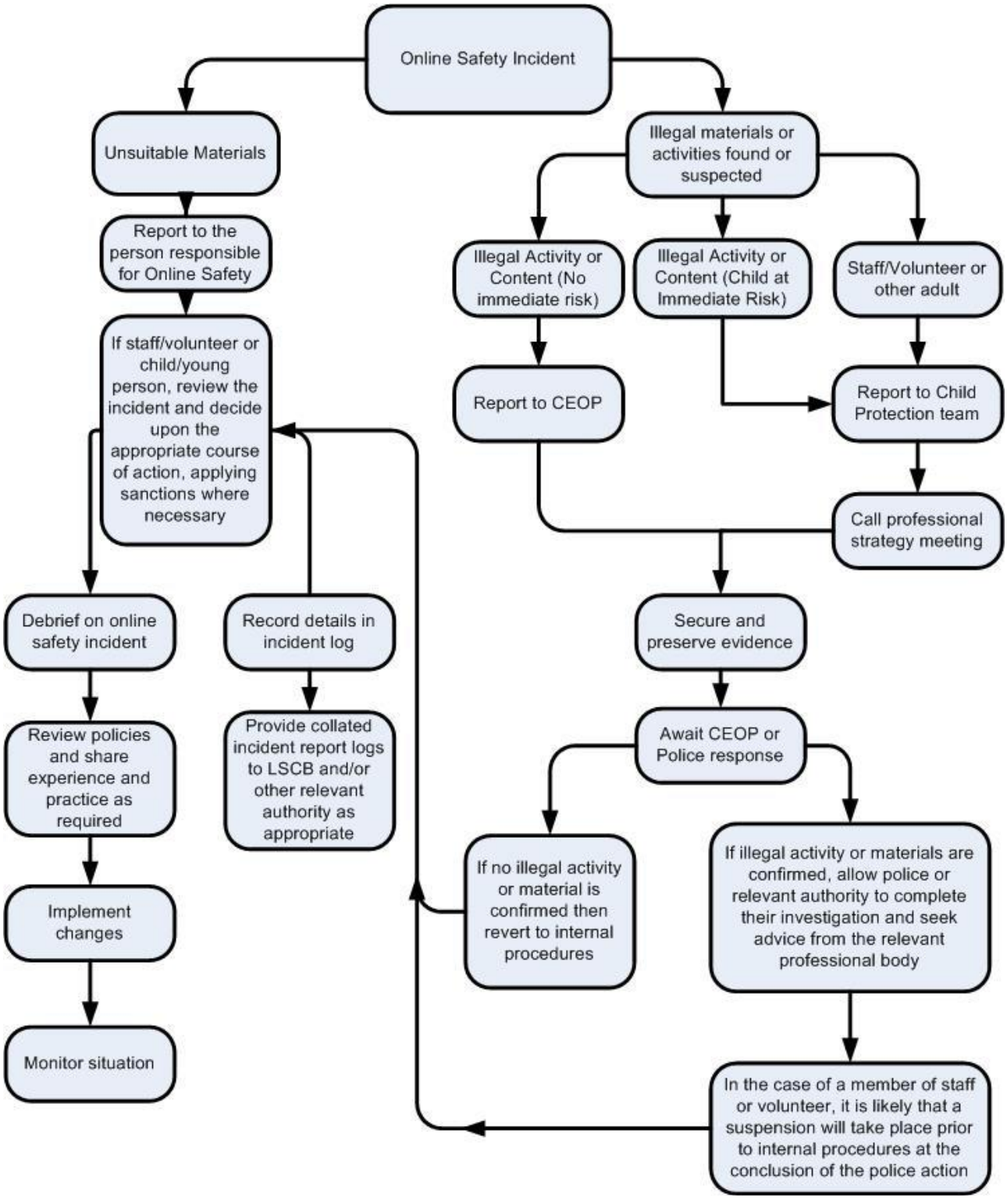
Inappropriate material (see ICT Acceptable Use Agreement)

- All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the class teacher.
- Deliberate access to inappropriate materials by any user will lead to the incident being logged by the class teacher/Head Teacher, depending on the seriousness of the offence; investigation by the Head Teacher/ LA, immediate suspension, possibly leading to dismissal and involvement of police for illegal offences. Any illegal activities (e.g. Child abuse images, grooming, and possession of pornographic images or criminally racist material) will be instantly reported to the police.

- Users are made aware of sanctions relating to the misuse or misconduct.

Illegal Incidents

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right hand side of the Flowchart (below and appendix) for responding to online safety incidents and report immediately to the police.



Equal Opportunities

<u>Pupils with additional needs</u>

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 ICT 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
    - 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.

ICT Acceptable Use Agreement (AUA)

POLICY STATEMENT

The Governing Body recognises the use of ICT as an important resource for teaching, learning and personal development. It actively encourages staff to take full advantage of the potential for ICT 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 ICT systems for work-related purposes, the Governing Body permits staff limited reasonable personal use of ICT 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 ICT 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 ICT 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.

E-mail and Internet usage

The following uses of the school's ICT 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.*

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 or brings the school into disrepute*

5. *for threatening behaviour including promotion of physical violence or metal harm*

6. *for the publication and distribution of personal data without either consent or justification*

7. *where the content of the e-mail correspondence is unlawful or in pursuance of an unlawful activity, including unlawful discrimination*

8. *to participate in on-line gambling*

9. *where the use infringes copyright law*

10. *to gain unauthorised access to internal or external computer systems (commonly known as hacking)*

11. *to create or propagate computer viruses or other harmful files*

12. *to enable or assist others to breach the Governors' expectations as set out in this policy*

Additionally, the following uses of school ICT 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 ICT facilities using another person's password, or to post anonymous messages or forge e-mail messages using another person's identity.*

Use of School ICT Equipment

Users of school ICT equipment:

1. *must not share and must treat as confidential any passwords provided to allow access to ICT equipment and/or beyond firewall protection boundaries*

2. *must report any known breach of password confidentiality to the Headteacher or nominated ICT 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 ICT systems*

4. *must not install software on the school's ICT systems, including freeware and shareware, unless authorised by the school's ICT Co-ordinator or Head Teacher*

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

Regulation of Investigatory Powers Act 2000

Ancillary to their provision of ICT 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.

Appendix 1:

Bampton CE Primary School's Staff, Governor and Visitor
Acceptable Use Agreement / ICT Code of Conduct

- I have read the e-safety policy document and the Acceptable Use Agreement on pages 9 and 10.
- I appreciate that ICT includes a wide range of systems, including mobile phones, PDAs, 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 an offence to use a school ICT system and equipment for any purpose not permitted by its owner.
- I will only use the school's email / Internet / Intranet and any related technologies for uses permitted 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 ensure that all school generated electronic communications are appropriate and compatible with my role.
- I will only use the approved, secure email system(s) for any school business
    - I will ensure that all data is kept secure and is used appropriately and as authorised by the Head teacher or Governing Body. If in doubt I will seek clarification. This includes taking data off site.
    - At school, I will not install any hardware or software without the permission of the HeadTeacher.
    - I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
    - Images will only be taken, stored and used for purposes in line with school policy and with written consent of the parent, carer or adult subject. Images will not be distributed outside the school network without the consent of the subject or of the parent/carer, and the permission of the Head teacher.

- I understand that my permitted use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to the Head teacher.

- I will respect copyright and intellectual property rights.

- I will not jeopardise the safety or wellbeing of any child or adult in the school through my use of ICT.

- I will not engage in internet behaviour which may bring the school into disrepute

- I will report any incidents of concern regarding children's safety to the Senior Designated Professional or Head teacher.

User Signature

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

Full name:……(printed)

Role:……

Signature:……**Date:**……

Appendix 2:

Bampton CE Primary School's E-safety agreement form for parents and carers.

Parent / guardian name:……..

Pupil name: ……

Pupil's class: ……

As the parent or legal guardian of the above pupil(s), I grant permission for my child to have access to use the Internet, school Email and other ICT facilities at school.

I know that my daughter or son has signed a form to confirm that they will keep to the school's rules for responsible ICT use and understand that my son/daughter may be informed if the rules have to be changed during the year. I know that the latest copy of the E-Safety Policy is available from the school office or on the school website and that further advice about safe use of the Internet can be found it the school's website.

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 a filtered internet service, secure access to email, employing appropriate teaching practice and teaching e-safety skills to pupils.

I understand that the school can check my child's computer files, and the Internet sites they visit. I also know that the school may contact me if there are concerns about my son/daughter's e-safety or e-behaviour.

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 e-safety.

Parent's signature:…… **Date:**……

Appendix 3:

Bampton CE Primary School's E-safety Rules

These E-safety Rules help to protect students and the school by describing acceptable computer use.

- I understand the school owns the computer network and can set rules for its use to keep me safe.
- I will only use ICT systems in school, including the internet, email and digital pictures for school purposes.
- I will only log on with my own user name and password.
- I will not share my passwords with anyone.
- I will only use my school email address at school.
- I will make sure that all messages are responsible, respectful and sensible.
- I will be responsible for my behaviour when using the Internet/learning platform. This includes resources and the language I use.
- I will not give out any personal information about myself or anyone else when using the internet.
- If I accidentally come across any material that makes me uncomfortable I will report it to a teacher.
- I will not download or install software.
- I will respect the privacy and ownership of others' work on-line at all times.
- I understand the school may watch my use of the school's computer systems and learning platform.
- I understand that I will only be allowed to use the school equipment and systems by following these rules.

Pupil name: ……

Pupil signature:…… **Date:**……