# Bluecoat C of E Primary School
# Great Torrington

# E-safety Policy

# GREAT TORRINGTON BLUECOAT C OF E PRIMARY SCHOOL

# E-SAFETY POLICY

**This policy was adopted by the Governing Body on** **5th February 2015**

**The policy will be reviewed on** **February 2017**

**Introduction**

At Bluecoat C of E Primary School we have a commitment to educating all stakeholders in the benefits of the use of ICT. High priority is given to recognising and managing the risks associated with the use of ICT in terms of e-safety and ensuring that all usage is appropriately and adequately controlled. This policy has been compiled in line with the guidance available from the SWGfL (see Links to other policies and legislation)

**What is the purpose of this policy?**

The purpose of this policy is to set out agreed principles and practice relating to e-safety within our school. All stakeholders, including staff, children, parents/carers, volunteers, visitors and community users are expected to be familiar with, and adhere to this policy. This policy is available from the school office, on the staff shared drive and on the school website.

Through implementation of this policy we will:

- Establish roles and responsibilities for stakeholders
- Educate all stakeholders in the effective and appropriate use of ICT in terms of risk management
- Establish consistent expectations regarding the appropriate conduct of all ICT users and outline procedures for Acceptable Use
- Ensure school systems are fit for purpose, appropriately set up to minimise risk and adequately monitored in line with guidance from SWGfL
- Establish clear systems for monitoring and responding to incidents causing concern in relation to e-safety
- Ensure that guidance on Data Protection from Devon County is adhered to ..link to policy
- Help children become confident and responsible ICT users appropriately equipped to manage e-safety and understand associated risks

These priorities will be underpinned by a positive and proactive approach to the use of ICT …curriculum …promoting independence in risk assessment

**Roles and Responsibilities**

Governors:

- Are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. Governors will receive regular updates regarding any e-safety incidents and monitoring reports.
- Will respond to reports of inappropriate use, investigating matters as appropriate and following school conduct procedure as necessary.

Headteacher/Senior Leadership Team:

- Has a duty of care to ensure the safety (including e-safety) of members of the school community.
- Should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff. See flow chart: “Responding to incidents of misuse” and relevant Local Authority HR disciplinary procedures.
- Is responsible for ensuring that relevant staff receive suitable training to enable them to carry out their e-safety roles and to train other colleagues, as relevant.
- Will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal e-safety monitoring role.

Safeguarding Officer:

- Should be trained in e-safety issues and be aware of the potential for serious child protection/safeguarding issues to arise from the sharing of personal data; access to illegal/inappropriate materials; inappropriate contact with adults/strangers; potential or actual incidents of grooming; and cyber-bullying.

ICT Team:

- Comprises an ICT Team & KS2 Lead, KS1 ICT Lead, ICT Curriculum & Admin Support and ICT Technical Support.
- Will meet regularly and have an overview of e-safety across the school, including policy and documents, filtering, curriculum provision, monitoring incident logs and monitoring improvement actions identified through use of the 360 degree safe self-review tool.
- Will ensure that the ICT managed service provider carries out all necessary e-safety measures

ICT Technical Support:

- Will ensure the technical infrastructure of the school is secure and not open to misuse or malicious attack, and monitor/report any misuse or attempted misuse.
- Will ensure that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed
- Will ensure the filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of one person.
- Will keep up to date with e-safety technical information ensuring the school meets e-safety requirements, informing and updating others as appropriate.

Staff:

- Will ensure they have up to date awareness of e-safety matters and are familiar with the e-safety policy and procedures.
- Will agree and sign the staff Acceptable Use Agreement.
- Are responsible for ensuring children have a good understanding of and are adhering to e-safety and Acceptable Use policies and will follow procedures for reporting any suspected misuse or problem.
- Will ensure that any digital communications with pupils/parents/carers is on a professional level and carried out using official school systems.
- Will monitor the use of digital technologies, mobile devices, cameras etc in lessons and school activities.

- Will ensure that where internet use is pre-planned pupils are guided to sites checked as suitable for their use and will report any unsuitable material found in internet searches

Pupils

- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- Will agree and sign the pupil Acceptable Use Agreement and understand the relevance of the document.
- Should understand the importance of adopting good e-safety practice when using digital technologies out of school

Parents & Carers

- Play a crucial role in ensuring that their children understand the need to use internet/mobile devices in an appropriate way.
- Will be encouraged to support the school in promoting good e-safety practice and to follow guidelines on the appropriate use of digital/video images taken at school events; parental sections of the website/VLE and online pupil records; and their children's personal devices within school.
- Will be supported to understand issues relating to e-safety through parent's evenings, newsletters, letters, website and information about national and local campaigns or literature.

Community Users

- Will be expected to sign and adhere to a Community User Acceptable Use Agreement prior to access being granted.

**How do we educate stakeholders in the appropriate use of ICT?**

Governors

Governors should take part in e-safety training/awareness sessions; this is of particular importance for those who are members of any committee involved in technology, e-safety, health and safety or child protection. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority/National Governors Association /or other relevant organisation (e.g. SWGfL).
- Participation in school training/information sessions for staff or parents which may include attendance at assemblies/lessons.

Pupils

The education of pupils in e-safety is an essential part of our e-safety provision. Whilst regulation and technical solutions are very important, at Bluecoat C of E Primary School their use will be balanced by educating pupils to take a responsible approach, supporting and encouraging them to be confident ICT users. They will receive the help and support of the school to recognise and avoid e-safety risks and build their resilience. Staff will reinforce e-safety messages across the curriculum, which will be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned e-safety curriculum will be provided as part of the overall planned curriculum
- Key e-safety messages will be reinforced as part of a planned programme of assemblies and other pastoral activities.
- Children will be taught in all relevant lessons to be discriminatory and critically aware of the materials/content they access on-line and be guided to validate the accuracy of information.
- Pupils will be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- Pupils will be helped to understand the need for the Pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside of school.

- Staff will act as good role models in their use of digital technologies the internet and mobile devices.
- In lessons where internet use is pre-planned, children will be guided to sites checked as suitable for their use and processes will be in place for dealing with any unsuitable material that is found in internet searches.
- Where pupils are allowed to freely search the internet, staff will be vigilant in monitoring the content of the websites the children visit.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the relevant designated person can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need. All staff involved are jointly and severally responsible for reinstating any filters as soon as the period of study is over.

Staff/Volunteers

All staff will receive e-safety training to support them in understanding their responsibilities, as outlined in this policy. Training will be offered as follows:

- All new staff will receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and Acceptable Use Agreements.
- Members of the ICT team will receive regular updates through attendance at external training events (e.g. from SWGfL/LA/other relevant organisations) and by reviewing guidance documents released by relevant organisations. They will then provide advice/guidance/training to individuals as required
- An audit of the e-safety training needs of all staff will be carried out regularly.

Parents and Carers

We recognise that many parents and carers have only a limited understanding of e-safety risks and issues, yet they play an essential role in the education of their children and in the monitoring and regulation of the children's on-line behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond. The school will therefore seek to provide information and awareness to parents and carers through curriculum activities, letters, newsletters, website, parent/carer's evenings, local and national e-safety campaigns.

Community Users

The school will provide opportunities for groups and members of the community to gain from the school's e-safety knowledge and experience. This may be offered through information on the school website; providing family learning courses in use of new digital technologies, digital literacy and e-safety; and supporting community groups, e.g. childminders and pre-schools to enhance their e-safety provision.

**How do we establish consistent expectations regarding the appropriate conduct of ICT users (incorporating Social Media)?**

Bluecoat C of E Primary School has a set of clear expectations and responsibilities for all users which are outlined in the relevant Acceptable Use Agreements (see appendices). All users are required to sign an agreement prior to access to the network being granted. The school adheres to the Data Protection Act principles and all users are issued with a username and password which should not be shared. All network systems are secure and access for users is differentiated.

With an increase in use of all types of social media for professional and personal purposes, it is essential that reasonable steps are in place to minimise the risk of harm to pupils, staff and the school through limiting access to personal information. Filtering is in place to restrict access to these sites on school premises and use of social media for professional purposes will be checked regularly. Clear guidance is issued to all staff on the use of social media outside of school:

School staff should ensure that:

- No reference is be made in social media to students/pupils, parents/carers or school staff
- They do not engage in online discussion on personal matters relating to members of the school community
- Keep passwords secret and protect access to accounts
- They do not befriend pupils or other members of the school community on social networking sites (careful consideration should be given to the implications of befriending parents or ex-pupils)
- Personal opinions are not attributed to Bluecoat C of E Primary School, Children's Centre or local authority
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information

**How do we ensure school systems are fit for purpose, monitor ICT use and respond to incidents causing concern?**

The school has a managed ICT service provided by an external contractor which is overseen by the ICT team. We recognise the importance of ensuring that the infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are fully implemented.

- There will be regular reviews and audits of the safety and security of the school technical systems.
- Servers, wireless systems and cabling must be securely located and physical access restricted.
- All users will have clearly defined access rights technical systems and devices.
- All users at KS2 and above will be provided with a username and secure password by the ICT Support staff who will keep an up to date record of users, their usernames and passwords. Users are responsible for the security of their username and password and passwords will be changed every year. Network access and email account passwords will be retained by the school to minimise administrative time.
- Group or class log-ons and passwords will be used for KS1 and below.
- The administrator password(s) for school ICT system must be available to the Headteacher and kept in a secure place.
- In order to maintain the integrity of the ICT infrastructure, teachers and support staff shall not have administrative access to computers or the network. Programmes shall not be installed on school computers, except by ICT technical staff.
- ICT Technical staff are responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations or users.
- Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by SWGfL by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored. There is a clear process in place to deal with requests for filtering changes.
- The school has provided differentiated user-level filtering to allow teachers to temporarily by-pass filters.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up-to-date virus software.
- Incidents, potential or actual, will be reported using the school Incident Form and any concerns relating to the misuse of ICT or breaches in security will be reported using the school Concern Form.  Reports will be monitored and investigated following school procedure.

**Data Protection**

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 and in line with our Data Protection Policy (see Links to Other Policies & Legislation).

**Links to other policies and legislation**

| Policies | Legislation |
|---|---|
| • SWGfL E-Safety Policy | • Data Protection Act 1998 |
| • Data Protection Policy | |

# Great Torrington Bluecoat C of E Primary School

## ACCEPTABLE USE AGREEMENT

**For Pupils in Foundation Stage and Key Stage One**

## This is how we stay safe when we use computers:

- I will ask a teacher or suitable adult if I want to use the computers or tablets.
- I will only use activities that a teacher or suitable adult has told or allowed me to use.
- I will take care of the computer, tablets and other equipment.
- I will leave the computer or tablet tidily and in a safe place.
- I will ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have done something wrong.
- I will tell a teacher or suitable adult if I see something that upsets me on the screen.
- I know that if I break the rules I might not be allowed to use a computer.

Signed (child): ……………………………………………

Signed (parent): …………………………………………..

# Great Torrington Bluecoat C of E Primary School

## ACCEPTABLE USE AGREEMENT

**For Pupils in Key Stage Two**

Digital technologies have become integral to the lives of children and young people, both in school and outside school. These technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

**This Acceptable Use Policy is intended to ensure:**

- that young people will be responsible users and stay safe while using the internet and other digital technologies for educational, personal and recreational use.
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and of users at risk.

The school will try to ensure that its children have good access to digital technologies to enhance their learning and, in return, expects its children to agree to be responsible users.

## Acceptable Use Policy Agreement

I understand that I must use school ICT systems in a responsible way, to help ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users.

**For my own personal safety:**

- I understand that the school will monitor my use of the systems, devices and digital communications.
- I will keep my username and password safe and secure – I will not share it, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will be aware of "stranger danger", when I am communicating on-line.
- I will not disclose or share personal information about myself or others when on-line (this could include names, addresses, email addresses, telephone numbers, age, gender, educational details, personal details or information, financial details etc.)
- If I arrange to meet people off-line that I have communicated with on-line, I will do so in a public place and take an adult with me.
- I will immediately report to a teacher or school adult any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.

**I understand that everyone has equal rights to use technology as a resource:**

- I understand that the school systems and devices are primarily intended for educational use and that I will not use them for personal or recreational use unless I have permission.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not use the school systems or devices for on-line gaming, on-line gambling, internet shopping, file sharing, or video broadcasting (eg YouTube), unless I have permission of a member of staff to do so.

**I will act as I expect others to act toward me:**

- I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.
- I will be polite and responsible when I communicate with others, I will not use strong, aggressive, impolite or inappropriate language and I appreciate that others may have different opinions to which they are entitled.

- I will not take or distribute images of anyone without their permission.

### I recognise that the school has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the smooth running of the school:

- I will only use my own personal devices (mobile phones / USB devices etc) in school if I have permission. I understand that, if I do use my own devices in the school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment.
- I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I try to use any programmes or software that might allow me to bypass the filtering and security systems in place to prevent access to such materials.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I will not open any hyperlinks in emails or any attachments to emails, unless I know and trust the person or organisation that sent the email, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes).
- I will not install or attempt to install or store programmes of any type on any school device, nor will I try to alter computer settings. If a setting is changed accidentally, I will report it to a teacher or adult as soon as possible.
- I will only use social media sites with permission and at the times that are allowed.
- I understand that I must not give information such as passwords, usernames or access details to anyone without permission and only for good reasons.

### When using the internet for research or recreation, I recognise that:

- I should ensure that I have permission to use the original work of others in my own work.
- Where work is protected by copyright, I will not try to download copies (including music and videos).
- When I am using the internet to find information, I should take care to check that the information that I access is accurate and appropriate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.

### I understand that I am responsible for my actions, both in and out of school:

- I understand that the school also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve my membership of the school community (examples would be cyber-bullying, use of images or personal information).
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I will be subject to disciplinary action. This may include loss of access to the school network/internet, suspension, contact with parents and in the event of illegal activities involvement of the police.

### I understand that school email addresses and accounts are only for school use:

- I understand that school email accounts are for use in school and for use at home when doing things directly connected with school. I understand that I must not use my school email address to sign up for any services of any kind unless I have permission from a teacher and it is for school purposes.
- I understand that although I can log in to school services and accounts from devices at home and elsewhere, I shall not upload anything that may cause problems for the school systems – such as files that are very large, files that contain inappropriate material or files that may contain viruses or other damaging content.
- I understand that I must not allow anyone else, including parents, carers and friends to use my email or other school accounts for their own purposes to communicate with anyone.
- I understand that the school must know my school account details including password(s) and that I must not change these without permission and without telling my teacher so that records can be kept up-to-date.
- I understand that my activity using school internet accounts is logged.

**Please complete the sections on the next page to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement, access will not be granted to school systems and devices.**

# Student / Pupil Acceptable Use Agreement Form

This form relates to the Pupil Acceptable Use Agreement, to which it is attached.

Please complete the sections below to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement, access will not be granted to school ICT systems.

I have read and understand the above and agree to follow these guidelines when:

- I use the school systems and devices (both in and out of school)
- I use my own devices in the school (when allowed) eg mobile phones, gaming devices USB devices, cameras etc
- I use my own equipment out of the school in a way that is related to me being a member of this school eg communicating with other members of the school, accessing school email, VLE, website etc.

| | |
|---|---|
| Name of Student / Pupil | |
| Group / Class | |
| Signed | |
| Date | |

# Great Torrington Bluecoat C of E Primary School

## ACCEPTABLE USE AGREEMENT

**For Staff and Volunteers**

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work.  All users should have an entitlement to safe internet access at all times.

**This Acceptable Use Policy is intended to ensure:**

- that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that staff are protected from potential risk in their use of ICT in their everyday work.

The school will try to ensure that staff and volunteers will have good access to ICT to enhance their work, to enhance children's learning and will, in return, expect staff and volunteers to agree to be responsible users.

## Acceptable Use Policy Agreement

I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users. I recognise the value of the use of ICT for enhancing learning and will ensure that children receive opportunities to gain from the use of ICT. I will, where possible, educate the young people in my care in the safe use of ICT and embed e-safety in my work with young people.

**For my professional and personal safety:**

- I understand that the school will monitor my use of the ICT systems, email and other digital communications.
- I understand that the rules set out in this agreement also apply to use of school ICT systems (eg laptops, tablets, email, VLE etc) out of school, and to the transfer of personal data (digital or paper based) out of school.
- I understand that the school ICT systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may see it or steal it.
- I understand that, as a general principle, school email and other online accounts should only be set up and used for school business and that personal email and online accounts are for personal business – any crossover should be avoided.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.
- I understand that at times I may use the 'safety filter bypass' to access online items for classroom use. When doing so I understand that I am personally responsible for continual monitoring of what is displayed by any computer, tablet or projector, I am using. I understand that it before leaving the computer all browsers must be shut down completely (in the case of some browsers, using a special shortcut to do so) in order to cancel the 'bypass'.

- I understand that I should only log on to school equipment using the login details provided for my use. Documents and materials to be shared with others should be copied to the shared area for others to access using their own login details.
- I understand that every time I leave a computer I should either log off as a user or I should temporarily lock the computer using, for example, the'Windows' key + L.
- I understand that I must use a secure password for my login to the school system and that my password should not be made available to anyone other than ICT support staff or senior staff of the school.
- I understand that any portable equipment, leads, chargers, power packs and other accessories are my individual responsibility in the case of loss or avoidable damage.

**I will be professional in my communications and actions when using school ICT systems:**

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital photographs and video images. I will not normally use my personal equipment to record these images, unless it is expeditious to do so – in which case they will be moved to the school system, and deleted from my equipment, before my equipment leaves the premises. Where these images are published (eg on the school website) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only use chat and social networking sites in school in accordance with the school's policies.
- I will only communicate with children, parents and carers using official school systems. Any such communication will be professional in tone and manner. I am aware of the risks attached to using my personal email addresses, mobile phones, social networking sites for such communications.
- I will not engage in any on-line activity that may compromise my professional responsibilities.

**The school and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:**

- When I use my mobile devices (laptops, mobile phones, tablets, USB devices etc) in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by the school about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- I will not use personal email addresses for any purpose on the school ICT systems.
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful content).
- I will ensure that my data is regularly backed up, in accordance with relevant school policies.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any unapproved means to bypass the filtering or security systems in place to prevent access to such materials.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- WiFi access codes, usernames and passwords must not be divulged to anyone not employed by the school. I will immediately report any instance where I believe someone not employed by the school has knowledge of any school usernames or passwords (including WiFi access codes).
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School Personal Data Policy (or other relevant policy). Where digital personal data is transferred outside the

secure local network, it must be encrypted. Paper based Protected and Restricted data must be held in lockable storage.

- I understand that data protection policy requires that any staff or child data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I will not use school email or other accounts to sign up to online accounts other than those directly related to my work in school. There should be a clear separation between all school related online accounts and all personal online accounts.

**When using the internet in my professional capacity or for school sanctioned personal use:**

- I will ensure that I have permission to use the original work of others in my own work.
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

**I understand that I am responsible for my actions in and out of the school:**

- I understand that this Acceptable Use Policy applies not only to my work and use of school ICT equipment in school, but also applies to my use of school ICT systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school.
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors or the Local Authority and in the event of illegal activities the involvement of the police.

I have read and understand the above and agree to use the school ICT systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Staff / Volunteer Name

Signed

Date

# Great Torrington Bluecoat C of E Primary School

## ACCEPTABLE USE AGREEMENT

**For Community Users**

**This Acceptable Use Agreement is intended to ensure:**

- that community users of school digital technologies will be responsible users and stay safe while using these systems and devices
- that school systems, devices and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that users are protected from potential risk in their use of these systems and devices

## Acceptable Use Agreement

I understand that I must use school systems and devices in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems, devices and other users. This agreement will also apply to any personal devices that I bring into the school.

- I will not use the school wireless Internet access except on business directly related to the school.
- I will not retain any password, nor will I reveal that password to any other person. I will remove or set my device(s) to 'forget' any WiFi or other internet access connection that has been set up on my device(s) immediately prior to leaving the school premises.
- I understand that my use of school systems and devices and digital communications will be monitored
- I will not use a personal device that I have brought into school for any activity that would be inappropriate in a school setting.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.
- I will not access, copy, remove or otherwise alter any other user's files, without permission.
- I will ensure that if I take and/or publish images of others I will only do so with their permission. I will not use my personal equipment to record these images, without permission. If images are published it will not be possible to identify by name, or other personal information, those who are featured.
- I will not publish or share any information I have obtained whilst in the school on any personal website, social networking site or through any other means, unless I have permission from the school.
- I will not, without permission, make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a school device, nor will I try to alter computer settings, unless I have permission to do so.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).
- I understand that if I fail to comply with this Acceptable Use  Agreement, the school has the right to remove my access to school systems.

I have read and understand the above and agree to use the school ICT systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Name

Signed

Date