Charlton Horethorne CE VA Primary School
Acceptable Use Policy

Staff and Volunteer Acceptable Use Policy

School Policy

This Acceptable Use Policy reflects the school online safety policy. The school will ensure that staff and volunteers will have access to technology to enable efficient and effective working, to enhance learning opportunities for pupils and will, in return, expect staff and volunteers to agree to be responsible users.

Scope of Policy

This Acceptable User Policy (AUP) policy applies to staff, volunteers and guests who have access to and are users of school technology systems, school related use of technology systems outside of school, and make use of social networks personally and professionally.

My Responsibilities

I agree to:

- read, understand, sign and act in accordance with the School online safety policy
- report any suspected misuse or concerns to the online safety leader
- monitor technology activity in lessons, extracurricular and extended school activities
- model the safe and effective use of technology
- demonstrate consistently high standards of personal and professional conduct especially in relation to use of social networks, making sure that these are in line with school ethos and policies especially at the time of a Critical Incident

Education

I agree to:

- provide age-appropriate online safety learning opportunities as part of a progressive online safety curriculum
- respect copyright and educate the pupils to respect it as well

Training

I agree to:

- participate in online safety training
- request training if I identify an opportunity to improve my professional abilities

Online bullying

I agree to:

- ensure the school’s zero tolerance of bullying. In this context online bullying is seen as no different to other types of bullying
- report any incidents of bullying in accordance with school procedures

Sexting

- I will secure and switch off any device discovered with an intimate sexting image and report immediately to the safeguarding lead.
- I will not investigate, delete or resend the image.

Prevent

- I will continually develop children’s ability to evaluate information accessed online.
- I will follow the agreed reporting procedure where children are purposefully searching for inappropriate sites or inadvertently accessing inappropriate sites.

Technical Infrastructure
I understand that the school will monitor my use of computers and the internet. I will not try to by-pass any of the technical security measures that have been put in place by the school which include:

- the proxy or firewall settings of the school network (unless I have permission)
- not having the rights to install software on a computer (unless I have permission)
- not using removable media e.g. memory sticks (unless I have permission)

Passwords

- I will only use the passwords given to me
- I will never log another user onto the system using my login

Filtering

- I will not try to by-pass the filtering system used by the school
- If I am granted special access to sites that are normally filtered I will not leave my computer unsupervised
- I will report any filtering issues immediately

Data Protection

- I understand my responsibilities towards the Data Protection Act and will ensure the safe keeping of personal and sensitive personal data at all times.
- I will ensure that all data held in personal folders is regularly backed up and kept secure.
- If I believe there has been a loss of personal or sensitive data, I will immediately report it to the Data Protection officer in the school.

Use of digital images

- I will follow the school's policy on using digital images, especially in making sure that only those pupils whose parental permission has been given are published.
- I will not use personal devices for taking or sharing digital images within school without the direct permission of the Headteacher. Where permission has been given, I will ensure that all digital images relating to school are removed from my personal device at the earliest opportunity.

Communication

- I will be professional in all my communications and actions when using school technology systems.
- I understand that I need to be open and transparent in all my communications.

Email

- I will use the school provided email for all business matters.
- I will not open any attachments to emails, unless the source is known and trusted (due to the risk of the attachment containing viruses or other harmful programmes).

Social Media and Personal Publishing

- I will ask permission before I use social media e.g. blogs, social networks or online communication tools with pupils or for other school related work.
- I will check with the SLT before I use sites/apps with learners to ensure that any pupil personal data is being held securely.
- I will follow the online safety policy concerning the personal use of social media.
- On any personal accounts I will not post any comments about any pupil and not post disparaging remarks about my employer/colleagues.
- When there is a Critical Incident, I will not post any comments online. **Mobile Phones**
- I will not use my personal mobile phone during contact time with pupils.
- I will not use my personal mobile phone to contact pupils or parents.

Reporting incidents

- I will report any incidents relating to online safety to the online safety leader.
- I will make a note of any incidents in accordance with school procedures.
- I understand that in some cases the Police may need to be informed.

Sanctions and Disciplinary procedures

- I understand that there are regulations in place when pupils use technology and that there are sanctions if they do not follow the rules.
- I understand that if I misuse the School technology systems in any way then there are disciplinary procedures that will be followed by the school.

I have read and understand the full School online safety policy and agree to use the school technology systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) in a responsible and professional manner as outlined in that document.

Staff/Volunteer Name ____

Signed ____

Date ____

Pupil Acceptable Computer and Internet Use Policy

Technology is a great tool to find information and to communicate and share with others.

The School encourages its appropriate, effective and safe use.

All users of technology in the school must agree to certain rules and will only use the

My Responsibilities
I understand that I have rights and responsibilities in using technology and will act responsibly when using technology, computers or the internet.

I will report any suspected misuse or problems to a teacher.

I will make sure I have permission to use any material that I find.

I will make sure that I maintain a healthy lifestyle by not spending too much time using technology.

Online bullying
I understand that the school will not accept bullying in any form.

I will be careful with all communications making sure that anything I write cannot be mistaken as bullying.

I understand that I should report any incidents of bullying.

Access to Internet Sites
I will not try to access sites that are blocked or that are unsuitable for use in school.

Communication – email, social networks, blog etc.
I will be careful in my communications making sure that nothing I write is offensive or may cause hurt or embarrassment.

I will not write anything that could be seen as insulting to the school.

Mobile Phones
I will only use my mobile phone as directed by my teachers.

Responsibilities
I understand that the school will monitor my use of computers and other technology.

I understand that the school may investigate incidents that happen outside school.

I understand that there are regulations in place when pupils use technology and that there are consequences if I do not follow the rules.

Name ____

Signed ____

Class ____________________ Date ____________________

Pupil/Parent Acceptable Use Policy

The internet will be used within school to support children’s learning both formally (within taught lessons) and informally (outside taught lessons), at the discretion of a member of staff who will set guidelines and rules for its use. Pupils will be taught to be critical and discriminating in their use of internet sites and to maintain a balance between the use of technology and other activities.

Pupils may have opportunities to communicate with others through blogs, communication tools, publishing work to online galleries and email. This will only take place in accordance with the school’s policy and procedure. Responsible and considerate language will be used at all times in communicating with others.

Pupils will:

- only use the school technology systems for those activities which they have been given permission to use and under the appropriate supervision of a member of staff.
- use the internet within the school to support learning.
- be made aware of what online-bullying is and what to do if it happens.
- only use the user names and passwords they have been given.
- not download and use material or copy and paste content which is copyright or not covered by the school copyright licenses.
- not attempt to search for, view, upload or download any material that is likely to be unsuitable in a school or is blocked by the school’s filter.
- inform a member of staff if they have accidentally accessed inappropriate content.
- use responsible and considerate language in communicating with others.
- be encouraged to maintain a balance between the use of technology and other activities.
- be encouraged to discuss their use of the internet and those sites that are age specific especially Social Network sites.
- only use mobile phones when directed by staff.
- be encouraged to talk with their parents or carers about the rules for the safe use of the internet.
- be made aware that the school may investigate incidents that happen outside of school but could have an effect on the school.

Failure to comply with these rules will result in one or more of the following:

- A ban, temporary or permanent, on the use of the internet at school.
- A letter informing parents of the nature and breach of rules.
- Appropriate consequences and restrictions placed on future access to school facilities.

Parents should:

- discuss online safety issues with their children
- maintain responsible standards when using social media to discuss school issues, and ensure that any issues of concern are raised with the school directly.
- inform the school if they think there is an online safety issue related to the school

If you do not understand any part of this document, please ask a member of staff for guidance. You should only sign the Parental Permission Form when you have read, understood and have explained the importance of these rules to your son or daughter.

The form below must be completed, signed and returned to the school for our records.
Use of the Internet may be withheld unless this has been done.

____

I have read, understood and explained the Acceptable Use Policy to my child and I am happy for my child to experience the Internet use described:

Pupil Name (PLEASE PRINT) ________________________________ Class __________

Name of Parent or Carer (PLEASE PRINT) ____

Signature of Parent or Carer ______________________________ Date __________

Technician/Administrator Acceptable Use Policy Extension

The school ICT Technician or person with administration rights is placed in an exceptional position of trust. Many of the duties that the Headteacher expects these people to complete could be against the Staff Acceptable User Policy of the school.

This document is not a job description but an addition to the Staff Acceptable User Policy that allows the ICT technician to fulfil these duties. Schools should customise this document to fit their needs.

Areas of concern are that:

- Files may be created, imported or processed by staff and pupils and stored on the school's servers or other storage systems (e.g. USB memory sticks, SD cards etc.) that might be of an inappropriate nature to the school setting. Inappropriate use includes any production, processing or transmission of offensive, provocative, extremist, racist, unethical, irreligious or anti-social materials in any format. Also included in this area are any materials that are against the rules and conditions of service for the school e.g. material that might bring the establishment into disrepute. Work created during the school's time or on the school's equipment or on one's own equipment but for school work, belongs to the school.

- User accounts will need to be created and serviced meaning that there may be access to these accounts by the ICT technician.

- Through work within the school's administration network the ICT Technician may be placed in the position of assisting in the processing of sensitive personal data including children's health or MIS data, confidential letters or information from or to senior staff, budgeting plans etc.

- The ICT technician, through specific user names and passwords, has control (sometimes through remote workstations) to the school's network. In the past there have been examples where these powers have been abused.

Because of these areas of concern the ICT Technician should:

- be responsible for monitoring the school's network.

- be given permission to access other user's files.

- protect the users by maintaining a filter for the school.

- monitor the internet use of users within the school.

- be aware of the laws relating to the use of computers especially those around Data Protection, Prevent and intimate Sexting images, copyright and those referred to in the school's Online Safety Policy and AUPs.

- make sure that they record all user names and passwords for all the services they access in a place where the senior leaders in the school can access them.

- have their use of the school's network, internet and other aspects of their work open for scrutiny.

To enable them to discharge these duties they should:

- receive training on the sensitive nature of their job especially in relation to Data Protection and the confidentiality of information and the school's Prevent duty.

- have an agreed procedure for managing the internet filter. This should include a log of decisions made and actions taken.

- have an agreed understanding of what is expected of them as far as the regular monitoring of the network system and internet

- have agreed procedures for reporting incidents.

- log any incidents including minor ones that are quickly resolved.

- be careful to make sure that they are observed when investigating serious incidents to make sure that they are protected against any allegations that could arise including:
  - secure and switch off any device that is suspected of containing an intimate sexting image and report to safeguarding lead
  - never open websites that are suspected of having inappropriate material unless others are present

- have frequent meetings with their line manger to report on any issues or trends.

As an ICT Technician (or a person who has administration responsibilities) I have read the above document and understand that I will be directed by senior staff to complete work outside of the Staff Acceptable User Policy.

I will report all concerns I have to the appropriate member of Senior Management.

Name: ____

Signed: ____

Senior Member of Staff: ____

Date: ____________________

Regular Visitor Acceptable Use Policy

Visitors will

- apply appropriate standards when using computing devices in school including an awareness of Data Protection, Copyright laws, Prevent duty and reporting.
- refrain from any use of your personal mobile phone or other device during the working day without permission of the Headteacher.
- not publish any information online that may be offensive to staff or pupils, or may bring the school into disrepute.

Logging in

- If you use the school's equipment, then request a guest log in.
- If you are using equipment that has been logged in by a member of staff always ensure a member of staff is present. Always lock the machine if they need to leave the room.
- If your service contract (Network/MIS support) allows you access to the system through team logins inform the school how you will be accessing the system.

Wireless Access

- Request permission to use the wireless connection (if available) asking for an authorisation key. You may need to change proxy settings.
- Remember that bandwidth is limited so avoid intensive use such as large downloads.

Internet Access and uploading

- The school's internet connection is filtered so access might be denied to some sites. Seek permission to access sites that are unavailable through the schools normal filtering system. This might not be possible as changes to the filter can take some time.
- You are responsible for the sites that appear on any machine that you are using. Report any issues with the member of staff present.
- Never upload and install software or updates without permission from a member of staff.

If you use your own equipment:

- Make sure that you have permission from the school for its use
- Ensure it has up to date virus protection software installed.
- Ensure that you take care with trailing wires.
- Ensure that you can identify your equipment.
- Never leave your equipment unattended or in an unlocked room.

Downloading files or documents
For all files

- Never transfer files unless you have permission.
- Make sure that you clearly state the purpose for transferring these files.
- Make sure that the USB stick/external hard drive has recently been virus checked. Check to see if the school machine you would like to transfer files from or to is encrypted as it might automatically encrypt your USB stick/hard disc drive.

If the file contains sensitive personal data such as staff or student information

- Get permission for this in writing or by email.

  (Note: Where existing service contracts (Network/MIS support) indicate that this type of work will take place permission will not be needed).

- Use an encrypted memory stick or hard drive.
- Transfer the file only over a secure email connection.

If you take pictures, video or sound files then check

- That you have permission to capture these files.
- That the staff/children have all given their permission for these images/voices to be used.
- That if you intend to use these files in a public area (website, blog etc.) or for financial gain that you request this permission in writing or through email.

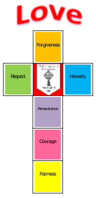
Reporting

- Report any incidence of accidental viewing of inappropriate images or materials.
- Report any incidence of deliberate searching for inappropriate images or materials.
- Switch off and secure any device that you suspect of containing an intimate sexting image and report immediately to the school's safeguarding lead.

Name ____ Date _______________________

Occasional Visitors online safety agreement

This list of statements has been developed with Beech Grove Primary School to use with visitors that are only in school for a one-off occasion such as, a supply teacher that isn't being used regularly by the school, a visiting speaker or students that are helping for single days.



On signing the visitors' book you agree to:

- only log onto the **school network** with the user name and password provided for you;
- inform the Headteacher or their representative if you intend to **use the internet**, asking permission before using any kind of social media with the children;
- refrain from any use of your **personal mobile phone** or other device during the working day;
- not taking any **photographs** without the specific permission of the Headteacher or their representative;
- report any suspected **misuse or concerns** about online safety whether by pupils or staff, to the Headteacher or their representative before leaving the school;
- not taking any **information on pupils or staff** off site unless specific permission has been given by the Headteacher or their representative;
- not **publishing any information** online that may be offensive to staff or pupils, or may bring the school into disrepute.

Bring Your Own Technology (BYOT)

As new technologies continue to change the world, they also provide many new and positive educational benefits for teaching and learning. To encourage this growth we are allowing people to bring their own technology into school and use them in lessons.

This Acceptable User Policy helps educate, inform people about the use of their technology on the school site.

Definition of technology
For purposes of BYOT, technology means any privately owned portable equipment such as tablets, laptops, netbooks, smart phones, cameras, any device capable of accessing the internet.

Internet
Only the internet connection provided by the school may be accessed while on the school site. Accessing the internet through a signal that does not go through the filtered access provided by the school is not allowed at any time.

Security and Damages
Responsibility to keep the device secure rests with the individual owner. The school, nor its staff or employees, are liable for any device stolen or damaged on the school site. If a device is stolen or damaged, it will be handled through the school policies similar to other personal belongings. It is recommended that decals, other custom touches and UV markings are used to physically identify the device. Protective cases should be used as well. If the device is capable of being GPS tracked then this should also be activated.

BYOT Student Agreement
The use of technology to provide educational material is not a necessity but a privilege. A student does not have the right to use his or her laptop, mobile phone or other electronic device while at the school. When abused, privileges will be taken away.

Students and parents or guardians partaking in BYOT must adhere to the student code of conduct, as well as all other school policies, particularly the online safety policy and the associated Student Acceptable User policy.

Additionally, technology:

- Must be in silent mode on the school site and on school buses
- May not be used in tests or exams
- Must only be used to access files or computer or internet sites which are relevant to the curriculum. Games are not permitted

Students acknowledge that:

- The schools network filters will be applied to the internet connection and attempts will not be made to bypass them
- Their personal device is virus protected and is not capable of passing on infections to the schools network
- Hacking, damaging or by passing the school internet security procedures is against the school policies
- The school has the right to collect and examine any device that is suspected of causing problems, either technical or from abuse of other school policies
- Printing from personal laptop devices will not be possible

- Personal technology is charged prior to bringing it to school and runs off its own battery. Charging will not be possible during the school day

Bring Your Own Technology (BYOT) Agreement

Please read and sign the BYOT agreement. No student will be allowed personal technology devices unless the agreement is signed and returned.

Students, parents and guardians participating in BYOT, must adhere to all school policies.

Please read carefully and initial every statement

	Students take full responsibility for their devices. The school is not responsible for the security of personal technology. Personal devices cannot be left on school property before or after school hours
	Devices cannot be used during tests or exams
	Student must immediately comply with the teachers request to shut down or close devices. Devices must be in silent mode and put away when asked by teachers
	Personal devices must be charged prior to bringing them to school and run off their own batteries while at school
	To ensure appropriate network filters, students will only use the school internet connection and will not attempt to by-pass this
	Students must make sure that their device is virus protected and is not capable of infecting the school network
	Students realise that printing for personal devices will not be possible
	Students should not share their device with other students, unless they have written permission to do so
	The school retain the right to confiscate and examine any device
	The school will inform parents or guardians of any misuse and in some cases, if confiscated, only return the device to the parent or guardian

Please understand that the use of personal devices to support educational experience is not a necessity but a privilege. With respect of the rules, this privilege will benefit the learning environment as a whole. When rules are abused privileges will be taken away.

I understand and will abide by the above policy and guidelines. I further understand that any violation is unethical and may result in the loss of my technological privileges as well as other disciplinary action.

____ Student Name

____ Student Signature

_____________________ Date

____ Parent