

Birchwood Primary School Policy



Acceptable Use Policies

Document Reference Number (if already used)	
Title	Acceptable Use Policy
Policy Owner	Headteacher
Version	1.
Approved Date	18.11.25
Approving Body	Governing Body
Next Review Date	November 2027

Version Control

Version	Last Modified	Last Modified By	Document Changes
1.	07.11.25	Neil Coleman	Update to Mobile Phone and Smart Watch use

Table of Contents

- 1 Staff and Volunteer Acceptable Use Policy
 - 1.1 Desktop / Laptop
 - 1.2 iPad
- 2 Parent and Carer Acceptable Use Policy
- 3 Children's Acceptable Use Policy

This policy incorporates all aspects of acceptable use relating to ICT and equipment within our school. It outlines the expectations for all stakeholders when using the systems provided by school making it clear the purpose of the use and the systems for reporting if something goes wrong.

These policies will be issued to the relevant parties on an annual basis in January. Staff will be expected to complete the agreement in Smartlog, the school's online Health and Safety compliance system. Volunteers, parents and children will be asked to complete either a MS Form or a paper copy of their understanding of the policies outlined below.

1. Staff and Volunteer Acceptable Use Policy

The review and maintenance of this policy is responsibility of the Full Governing Body.

Aim: The aim of this policy is to protect the school's IT systems and electronic data from damage (e.g. through introduction of viruses) and unauthorised disclosure through inappropriate staff and volunteer use.

Purpose: To set out protocols, procedures and restrictions for acceptable use of IT systems by staff and volunteers of the school.

Relationship to other policies: The Staff and Volunteer AUP is part of the school Online Safety Policy and also relates to Data Protection.

School Policy:

This Acceptable Use Policy reflects the school Online Safety Policy. The school will ensure that staff and volunteers will have good access to ICT to enable efficient and effective working, to enhance learning opportunities for children and will, in return, expect staff and volunteers to agree to be responsible users.

Scope of Policy:

This Acceptable User Policy (AUP) applies to staff, volunteers and guests who have access to and are users of school ICT systems and to school related use of ICT systems outside of school.

My Responsibilities

I agree to:

- read, understand, sign and act in accordance with the School Online Safety policy
- complete a CPOMS or safeguarding concern to report any suspected misuse or problems to the DSL and Computing / online safety Lead
- understand the risk of cyber security as a first line of defence against cyber incidents and attacks.
- monitor ICT activity in lessons, extracurricular and extended school activities
- model the safe use ICT

- refrain from publishing any information that: may be offensive to colleagues, may breach the integrity of the ethos of the school or may bring the school into disrepute (this includes personal sites)

Education

- I understand that I am responsible for the Online Safety education of children
- I will respect copyright and educate the children to respect it as well

Training

- I understand that I will participate in Online Safety training (MB Digital enrichment lead)
- I understand that I will participate in Cyber Security training (Secure Schools)
- I understand that it is my responsibility to request training if I identify gaps in my abilities

Cyberbullying

- I understand that the school has a zero tolerance of bullying. In this context cyberbullying is seen as no different to other types of bullying.
- I understand that I should report any incidents of bullying in accordance with school procedures

Technical Infrastructure

I will not try to by-pass any of the technical security measures that have been put in place by the school. These measures 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 (unless I have permission)

Passwords

- I will only use the password(s) 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
- I understand that the school will monitor my use of computers and the internet

Data Protection

- I understand my responsibilities towards the Data Protection Act and will ensure the safe keeping of personal data at all times.
- I will ensure that all data held in personal folders is regularly backed up.
- I will not carry data that uses personal information about anyone on an unprotected hard drive
- I will use the password protected external hard drive provided by school for all work related to school (teachers only)

Digital Images

- I will follow the school's policy on using digital images making sure that only those children whose parental permission has been given are published
- I will not use full names to identify people

Communication

I will be professional in all my communications and actions when using school ICT systems.

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

- I will ask permission before I use social media with children or for other school related work

Personal publishing

- I will follow the Online Safety policy concerning the personal use of social media

Mobile Phones and wearable technology

- I will not use my personal mobile phone / smart tech during contact time with children
- I will not use my personal mobile phone to contact children or parents with the exception of school trips where the Headteacher must be informed of their use.

Reporting incidents

- I will complete the school's concern sheet to report any suspected misuse or problems to the Online Safety Leader
- Complete a CPOMS or safeguarding concern to report any suspected misuse or problems to the DSL and Computing / online safety Lead
- I will report any potential cyber security risks to the Digital Enrichment lead or Headteacher
- I will follow Child Protection procedures for all serious concerns
- 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 children use ICT and that there are sanctions if they do not follow the rules.
- I understand that if I misuse the School ICT systems in any way then there are disciplinary procedures that will be followed by the school.

Acceptable Use Agreement

I have read, understood and agree to abide by the terms of the Acceptable Use Policy.

Name:.....

Position:

Signature:..... Date:.....

Headteacher signature:..... Date:.....

(please complete and return this form to the school office)

1.1 Laptop Acceptable Use Policy for Teaching Staff

Laptops are issued to staff based on a number of expectations. It is important to highlight these to avoid any confusion in the future.

- The laptops are owned and issued by the school and loaned to staff as and when they become available and at the discretion of the Headteacher. Loan of a laptop is not 'a right'.
- The school will maintain and pay for any failure of the machine or software as a result of normal use/wear and tear subject to costs and budget available.
- Laptops are issued primarily for the end benefit of the children and for staff to be able to support teaching and learning in a specific classroom or classrooms.
- Staff laptops are for use **only** by school employees.
- Staff laptops are not to be used directly by children who should use the school based laptops.
- Laptops may be taken out of school and used at home. They must be carried in a proper laptop case to protect the computer during journeys. However, once off school property, it is expected that staff are responsible for the laptop. Any accidental damage, occurrence of theft etc occurring outside school property is the responsibility of the person loaned the laptop. (It is strongly advised that the laptop is insured by means such as ones own 'house hold insurance'. They may NOT be left in vehicles unattended)
- Additional software, other than that approved by the school is loaded onto a computer at 'own risk'. (ALL software should be licensed and must be removed on final return of laptop)
- Use of the Internet via the school lap top on/off site should always comply with the school's 'user agreement'/Online Safety policy.
- Since the laptop is to support children's learning; for periods of extended absence (i.e. 10 days or more) laptops are returned to school, unless an alternative arrangement has been made with the Headteacher.
- Following a period of loan, laptops should be returned to the school in condition they were given (less reasonable wear and tear).
- The laptop is loaned on the understanding that all due care and attention is taken over confidential information e.g. sensitive files are password protected or stored on a 'pen drive' or 'cloud' which is kept securely.

Laptop Acceptable Use Agreement

I have read, understood and agree to abide by the terms of the Laptop Acceptable Use Policy.

Laptop Serial Number:.....

Laptop Asset Number:.....

Name:.....

Position:

Signature:..... Date:.....

Headteacher signature:..... Date:.....

(please complete and return this form to the school office)

1.2 iPad Acceptable Use Policy for Teaching Staff

Introduction

The aim of the Acceptable Use Policy (AUP) is to ensure that all staff are aware of their professional responsibilities in relation to iPads provided for staff use by the school. This AUP is not intended to unduly limit the ways in which members of staff teach or use ICT, but aims to ensure that the school and all members of staff comply with the appropriate legal responsibilities, whilst the reputation of the school is maintained and the safety of all users is ensured. We expect staff to use their iPad in the classroom to enhance the teaching and learning experience for their pupils.

The iPads are to be used for professional purposes only and staff must bring their iPad to school every day, fully charged.

All users of the iPads will be required to review this AUP and sign the bottom of the form in order to demonstrate an understanding of these rules. iPad users will also agree to follow all relevant policies and procedures, be role models, display good practice and provide leadership in the use of these devices.

Teacher use of the iPad falls under the guidelines of Warwick Education Services' Acceptable Use Policy for technology. Access to the internet is monitored through our school's content filtering software and all rules and expectations are applied to the use of the iPad. All applications and documents stored on the iPad are the property of Birchwood School and are subject to regular review and monitoring.

Teachers will be provided with a 9th Generation iPad Model A2602 (64GB), USB Cable, lightning Charger and case. The iPad must be surrendered to Birchwood School in appropriate working condition, immediately upon termination of employment or at the request of the Head of School. Birchwood Primary School reserves the right to require the return of an iPad from a staff member at any time and without notice.

At all times the iPad shall remain the property of the school and is subject to all of the school's standard rules, policies and procedures concerning access to, and use of, the Internet and email.

Individual users are responsible for the setting up of any home internet connection to use in conjunction with the iPad and no support will be provided for this by the school.

The following guidelines are general in nature as not every possible scenario can be thoroughly described or known at this point in time.

Maintenance and Care of Devices

- Staff issued with an iPad are expected to exercise the same care in respect of the security and upkeep of the iPad as if it were the employee's own property.
- Malfunctions or any other technical problems (either hardware or software related) should be reported immediately to the Headteacher, so that steps can be taken to have the problem rectified by an approved technician as quickly as possible. Under no circumstances is the employee to organise repairs to the iPad before reporting the problem.
- Lending the iPad to any third party is strictly prohibited. Use of an organisation-owned iPad by the user's friends and/or family is also strictly prohibited.
- Careless loss, damage or misuse of the iPad, its case or any other associated peripherals may result in disciplinary action and, in cases of serious misconduct, may result in the employee's dismissal.
- Users must keep the iPad away from food and drink at all times.

- The iPad screens are particularly sensitive to damage from excessive pressure on the screen. Users must avoid placing too much pressure and/or weight (such as folders and workbooks) on the screen in order to refrain from any unnecessary damage.
- The iPad must not be subjected to extreme heat or cold.
- Users must keep the iPad clean and in good working order.

Security and Privacy

- It is a user's responsibility to keep their iPad safe and secure. When iPads are left unattended they must be locked in a secure cupboard in your classroom/school.
- It is a user's responsibility to ensure that their allocated iPad is securely locked away at night, whether at work or at home. Similar care must be taken when leaving the iPad in a meeting room, any off-site venue and whilst travelling.
- iPads must not be left unattended or on view in motor vehicles at any time.
- If the iPad is lost, stolen or damaged, the Headteacher must be notified immediately. If necessary, the device will be remotely locked and/or wiped. Birchwood School is not responsible for the loss of any personal files that may be deleted remotely from an iPad.
- The use of 'Jailbreaking' is strictly prohibited ('Jailbreaking' is the process which removes any limitations placed on the iPad by Apple, resulting in a less secure device).
- Users are required to set up a pin or pass code/password lock to keep the device protected. This code is strictly confidential and must not be divulged to staff or pupils.
- If you have enabled the facility on your iPad to receive and send school emails, you must ensure your iPad has a pass code/password lock in place.
- Along with the Acceptable Use Policy, staff must adhere at all times to the Data Protection Act (2018), The Computer Misuse Act (1990) and amendment (2022) and the school's health and safety policy when using iPads in school.
- In order to prevent access to confidential information, staff iPads should never be used by pupils.
- Users may not use private emails to send content that, if intercepted, would place the school in violation of laws or regulations.
- Staff may not use the internet to view illegal or inappropriate material that would place the member of staff or school at legal risk.

Applications

- Selected applications installed on staff iPads must align with educational purposes. Purchase and installation of such apps must be made through the Headteacher.
- Individual members of staff are also allowed to purchase appropriate apps for themselves, using their own Apple ID, as long as they are in keeping with the school's Acceptable Use Policy. The cost of such apps will not be reimbursed.
- Apps which would benefit other members of staff can be requested via email to the Headteacher, who will be responsible for the app budget.
- Staff should be aware that the school, via its Apple device management system (Jamf), can see what apps are installed on each iPad.
- Where apps are required to be deployed to all staff iPads simultaneously, the devices will need to be returned to the school Technician.
- Updates to applications can be carried out by teaching staff, when required.
- Memory space is limited and academic content takes precedence over personal files and apps.

Social Media

- For the purposes of this policy, social media includes (but is not limited to) internet forums, blogs, wikis, podcasts, photograph websites (Snapchat, Instagram, WhatsApp etc.), Facebook and X. Staff should follow these guidelines in relation to any social media applications that they use, both in work and in their personal lives.

- Users should not access social media applications from the school's iPads when working in school unless it is for educational purposes, and is previously agreed and sanctioned by the Headteacher.
- Users should understand that anything they write (regardless of privacy settings) could be made public by other users. Staff should ensure they remain professional and ensure a clear distinction between professional and personal lives.

Use of Digital and Video Images

- Staff using iPads must be aware of the risks associated with sharing images and videos on the internet.
- Users must make good judgment when using the iPad camera. The user agrees that the camera will not be used to take inappropriate, illicit or sexually explicit photographs or videos, nor will it be used to embarrass anyone in any way.
- Staff must not take, use, share, publish or distribute images of others without their permission.
- Posting of images/movie on the Internet into a public forum is strictly forbidden, without the express permission of a member of the Senior Leadership team.
- Inappropriate media may not be used as a screensaver or background photo.
- Deletion of photos and videos may happen periodically by the Headteacher or if a device's memory is full.

iPad Acceptable Use Policy for Teaching Staff

I have read, understood and agree to abide by the terms of the iPad Acceptable Use Policy.

iPad Serial Number:.....

iPad Asset Number:.....

Name:.....

Position:

Signature:..... Date:.....

Headteacher signature:..... Date:.....

(please complete and return this form to the school office)

2. Parent and Carer Acceptable Use Policy

The review and maintenance of this policy is the responsibility of the Executive Leadership Team of the Community Academies Trust.

Aim: The aim of this policy is to provide parents and children with a common understanding of procedures to safeguard the children through appropriate, effective and safe use of the Internet and use of mobile devices.

Purpose:

- To set out for what purposes the Internet will be used in school
- To state the rules for child use of the Internet and mobile phones in school
- To state what will happen if these rules are broken.

Relationship to other policies: The Parent and Carer Acceptable Use Policy is part of the school Online Safety Policy and also relates to Data Protection.

The Internet offers both educational and social opportunities for our children. Whilst recognising the benefits we must also establish appropriate, effective and safe use of the Internet. 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. Children will be taught to be critical in their use of Internet sites.

Children may have opportunities to communicate with others through eSchools and blogs. This will only take place in accordance with the school's policy and procedure, so their full name will never appear online. Responsible and considerate language will be used at all times in communicating with others.

Children will:

- only use the school ICT 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 cyber-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 ICT 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 (SMART)
- 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 sanctions and restrictions placed on future access to school facilities.

If you do not understand any part of this document, you should ask a member of staff for guidance.

If you have any concerns regarding this policy, the form below must be completed, signed and returned to the school for our records.

Parent's name:	
Child's name	
School:	
Class:	
Date:	
Comments:	

3. Children's Acceptable Use Policy

Technology is a fantastic resource to support learning within school and to communicate with others. The School encourages its appropriate, effective and safe use. All users of technology and devices in school must agree to certain rules and will only use the equipment and software as instructed.

My Responsibilities

- I understand that I have rights and responsibilities in using ICT and will act responsibly when using technology, computers or the internet.
- I will learn the school's SMART rules to keep myself safe inside and outside of school
- I will report any suspected misuse or problems to a teacher or trusted adult within school.
- I will make sure there is permission to use any material that I find i.e. copyright

Communication – eSchools, email, social networks, blog etc.

- I will be careful in my communications making sure that nothing I write is offensive, and that it is considerate.
- I will not write anything that could be seen as insulting to the school.
- I understand that I should report any incidents of potential cyber security attacks

Cyberbullying

- 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 is considerate and could not be interpreted as bullying.
- I understand that I should report any incidents of bullying and know how to do this.

Policy Review Sheet

Please note any comments or suggested amendments on this sheet. You may also choose to complete your comments in confidence on a separate piece of paper. Please add your initial to any comments.
