INTERNET ACCEPTABLE USE POLICY

BEDSTONE COLLEGE

Last Reviewed	September 2022
Review Frequency	1 Yr
Review Date(s)	Sept 2024
Signed Off	T. Mullis

Contents

INTERNET ACCESS ACCEPTABLE USE POLICY 3
- Aims 3
- Cyberbullying 3
- Bystanders 3
- General 3
- Network Access 4
- E-mail and other Communication tools 4
- The Internet 5
- ICT Hardware 5
- Cyber Security 6
- Online Learning – where appropriate 6
- Screen Time 7
- Sanctions 8

Appendix 1: 9
- PARENT GUIDE 9
  - Your child's screen time 9
  - What's the problem? 9
  - 5 steps you can take to protect your child 9
  - How to set parental controls on your devices 11
- Microsoft devices (Windows computers and Xbox): 11
  - Set screen time limits 11
  - Set age limits for apps, games and media 11
  - Block inappropriate websites 11
  - Manage purchases in the Microsoft Store 12
- iPads and iPhones: 12
  - Set a screen time passcode 12
  - Block in-app purchases 12
  - Block explicit content and set controls on apps 12
  - Filter website content 13
- Fire Tablet 13
  - Set a parental controls password 13
  - Restrict apps, features and content 13
  - Block in-app purchases 13
  - Restrict available content 13
  - Set times when your child can use the tablet 13

Android phones 14

Set up parental controls 14

Restrict purchases 14

Manage screen time 14

PlayStation 14

Set a login passcode and system restriction passcode 14

Set spending limits 15

Restrict access to network features 15

Set age rating levels for games, Blu-ray Discs and DVDs 15

Sources used in this guide 15

INTERNET ACCESS ACCEPTABLE USE POLICY

Aims

This policy sets out acceptable use of the School network, the ICT equipment and access to the internet and e-mail facilities. All staff and pupils are required to adhere to the directives laid down in the policy and any breach may lead to disciplinary and/or legal action. The School reserves the right to monitor usage of the network, and pupils should be aware that routine monitoring will lead to the discovery of policy violations, in particular visits to inappropriate sites and the downloading or transmission of copyright material.

Annual reviews of this Acceptable Use Policy will be undertaken and amendments made to reflect changes in the services provided by the School, changes in UK law and the evolution of Information and Communication Technology in the wider sense. Both staff and pupils must ensure that they adhere to the current version of the AUP.

This policy should also be read in conjunction with the *School's Anti-Bullying Policy*, and the School's *Acceptable use policy for mobile devices*.

Cyberbullying

The School will not tolerate cyberbullying. Cyberbullying is defined as the use of information and communications technology (ICT), particularly e-mail, mobile phones and the internet, to deliberately upset someone else. It can take many forms, including threats, intimidation, harassment or cyberstalking by, for example, repeatedly sending unwanted messages or texts.

Cyberbullying is referred to in the School's general Anti-Bullying Policy and Cyber-bullying Policy.

Bystanders

In cases of cyberbullying bystanders, or 'accessories' to the bullying, often have a more active role,
e.g. forwarding messages or contributing to chat room discussions. Therefore although they may not have started the bullying they are active participants and often make the matter worse.

The School makes it clear to all pupils that bystanders have a key responsibility to the School community and to anyone they see being bullied or victimised. They are encouraged not to tolerate such behaviour and to stand up for what they know to be right, for example by telling a member of staff what they have seen or heard.

Access to the School's ICT resources is a privilege and continuance of this facility requires pupils to behave appropriately and to display a responsible attitude at all times.

General

The internet and related services are provided for students and staff at Bedstone College to further educational goals and objectives.

Each student and staff member is responsible for his/her behaviour and communications over the network. Users must abide by the School's general standards, including all safeguarding requirements, code of conduct, and the common courtesies.

Any use of the School ICT resources, including communications (e.g. e-mails, video conferencing) and storage of data (whether on a network resource or external storage media provided by the School, or accessed using the School's network) may be reviewed. Users cannot expect files on School servers or School provided cloud storage media to be private.

Network Access

All users must always use his/her own school issued account to access the network. Any attempt to impersonate another user or to interfere with data stored on the network by another user will be treated as a serious offence. Both these activities are illegal under UK law.

Passwords must be chosen carefully – they should not be readily 'guessable' – and kept secure. A password must never be divulged to others. If it is suspected that a password is known by other users, it must be changed immediately.

If a user identifies a potential security problem, he/she must notify a member of the ICT support staff immediately.

Students and staff must take every precaution to ensure that computer viruses are not introduced onto the network. **The use of VPNs (Virtual Private Network) are strictly forbidden,** and any user found to be using one to circumnavigate the Schools' internet filter will likely be removed from the network for a period of time, and face a disciplinary process.

E-mail and other Communication tools

All students and teaching staff are provided with a School email account and access to Microsoft Teams. Only the school account should be used for communication between staff and students. Students should not email or message their teachers using private accounts, and under no circumstances should a teacher email a student using their private account.

All e-mails and communication must be polite and use appropriate language. In particular they must not contain any material that could be considered abusive, sexist, racist or that incites hatred or is known to be simply untrue.

E-mails and Teams communication should not reveal personal details, whether about the sender or someone else, nor should they be used to arrange a meeting with someone known only via the internet.

Any pupil receiving an abusive or offensive e-mail or communication should inform a member of staff immediately. He or she should not respond to such messages.

Pupils should not engage in 'spamming' or participate in chain e-mails.

The use of e-mail or Teams chat for social purposes should be kept proportional to the primary academic purpose. Social e-mail or Teams chat is strictly forbidden during lessons without explicit permission of a member of staff.

E-mails sent to external recipients on behalf of Bedstone College must be carefully written and authorised by a member of staff BEFORE sending.

Use of, and access to, emails and Teams is the responsibility of the user, and all users should exercise full care and caution when accessing email accounts, and opening email attachments. If a user suspects that they may have accidentally opened a malicious email, they must notify the IT Support Team immediately.

The Internet

Viewing, retrieving, downloading or transmitting illegal or inappropriate material is prohibited, as is knowingly visiting websites where such material may be found. Any user discovering such sites accidentally should report the details to a member of if the IT support staff immediately.

Any user deliberately found to be accessing inappropriate material on any device within the School premises, or using school devices (including off-site) will be deemed to have transgressed either the Schools' Behaviour Policy (Students) or Staff Code of Conduct (All Staff). The School uses a Sophos filter to monitor all searches, access to websites on all devices, and regular reports are generated and passed to the Deputy Head, and DSL.

Intellectual property rights must be respected at all times. Users must not create and/or transmit material which infringes copyright. It is a breach of the School's plagiarism policy to pass off another's work as one's own and this extends to information obtained electronically. All internet sources must be acknowledged when producing pieces of work.

Use of the School's internet and ICT facilities for financial gain, advertising or other commercial activities is prohibited.

ICT Hardware

Users must respect the School's network infrastructure and ICT equipment, and take appropriate care when using it. Any damage, however caused, must be reported immediately to a relevant member of IT support staff.

Hardware must not be connected, disconnected or tampered with in any manner without explicit permission. This includes the use of any software or any app used to bypass the College's filters.

Unnecessary waste or abuse of ICT resources (for example inappropriate printing) may result in financial charges and/or suspension of network access.

Cyber Security

All staff are required to have multi-factor authentication (MFA) set up on their school account. This ensures that a user is only granted access to their account after successfully presenting two or more pieces of evidence to authenticate the account holder.

Students are being enrolled in MFA over the course of this academic year.

Online Learning – where appropriate

The School makes use of Schoolbase as a learning platform for the setting of prep tasks, and for providing student information including academic reports. Users are issued with a secure username and password, and should ensure that these remain private. Parents, Teaching Staff and Students are allowed access to appropriate parts of the platform for each user group.

Teams is an online video conferencing tool made available to teaching staff to support learning from home. The following points should be observed by all users:

- Only sessions facilitating group lessons should be hosted (no one-to-one sessions are permitted (except in respect of peripatetic staff and designated safeguarding leads as detailed below)
- Staff and students must wear appropriate suitable clothing, as should anyone else in the household
- Any computers or mobile devices used should be in appropriate areas, for example not in bedrooms; and where possible be against neutral background
- Microsoft OneNote and Teams may be used to provide structure and materials for lessons
- Live classes should as a general rule be limited to no more than twenty minutes to provide a reasonable length of time for all users, and to balance screen time with other activities (it is accepted that there may be legitimate exceptions such as a peripatetic music lesson)
- Language must be professional and appropriate as it would be within a classroom environment, including for any family members in the background
- Teachers hosting classes will continue to use the three-warning behaviour policy for low level disruption, upon which on the third warning students will be removed from the session and the issue reported to the Deputy Head. Significant disruption, rudeness, or inappropriate content result in the user being removed immediately from the session and the issue reported to the Deputy Head.
- Any user alarmed or concerned by any online Teams session (either for content, breach of this policy, or other worry) should immediately contact one of the Senior Management Team.
- All students clicking on a Teams link will be taken to a waiting room. Teachers (Hosts) will take class registers (and unsure appropriate and correct students are in the waiting room. Teachers (Hosts) will then admit participants to the main room; all participants will have their audio and video muted upon entry. These measures are in place for the security of all.

- All recordings of **live** sessions are protected under GDPR and stored on appropriate UK servers. They exist only for safeguarding purposes and not for further broadcast or transmission if students are included in the video recording. For example, a recorded session of a teacher demonstrating an example where no students are included would be acceptable for later use as a potential Schoolbase resource
- Teachers should be mindful as to the needs of their learners. Some students may find working in this manner difficult, and may have specific educational needs that must be considered. Teachers should therefore be flexible in their approach to using such mediums, and in ensuring that they meet the needs of their students
- The School manages the overall permissions and settings for Teams, and so will disable certain features for the adequate safeguarding of students.

Teaching staff (as appropriate) are provided with a School device for providing online learning, including the use of Teams to enhance the quality and engagement of their lessons. Teaching staff should not use their own personal devices for hosting Teams sessions with students.

The School's policy is to limit Teams sessions to a maximum of forty minutes per session as a general rule (with the exception of peripatetic teachers), and only one session within each 45-minute period.

Peripatetic teaching staff who ordinarily teach on a one-to-one basis are subject to the same points stated above in regards to online learning. It is therefore only possible for their lessons to be delivered online using live Teams sessions if they are run as a group (e.g. more than one-to-one) **or if the parent appears in the background at the start of the session to state that they will be monitoring in the background and that they are happy for the lesson to go ahead.** Peripatetic staff are self-employed professionals are therefore able to use an appropriate business device, and will deliver the normal length of lesson appropriate to each student.

*If the School is working remotely, the designated safeguarding leads of the School are able to host a one to one Teams session with students where there is a pastoral or safeguarding necessity to do so. However, all sessions are securely recorded and can be reviewed at a later date if for safeguarding reasons this were required.

Screen Time

Spending time online and on devices can be a positive thing. But, higher screen time can put students at more risk of encountering bullying online, abuse and grooming (when someone builds a relationship with a child to exploit or abuse them), seeing inappropriate content, and not getting enough sleep and exercise.

As a School we spend considerable time educating students on these risks through our PSHE programme, and on how to stay safe online with appropriate content delivered across the Junior School and Senior School. This includes offering periodic parental talks.

There is a great deal of advice for parents on how you can protect your child online, including how to set parental controls, age limits for apps, games and media, and use of gaming consoles. Further details are provided in ***appendix 1***.

Sanctions

The full range of School sanctions is available for dealing with students transgressing any of the above rules.

In addition, abuse may result in a temporary ban on internet/computer use, with parents being informed.

Staff should refer to the Code of Conduct.

Where contravention of the rules may involve a transgression of the law, the police or local authorities may be involved.

Appendix 1:

PARENT GUIDE

Your child’s screen time

If there’s a school closure or self-isolation due to coronavirus (COVID-19), your child will likely be spending more time on devices than usual, especially if doing remote learning. Know the risks, and what you can do to keep your child safe.

What’s the problem?

Spending time online and on devices can be a positive thing. But, higher screen time can put your child more at risk of:

- Being bullied online
- Abuse and grooming (when someone builds a relationship with a child to exploit or abuse them)
- Seeing inappropriate content
- Not getting enough sleep and exercise

5 steps you can take to protect your child

1. Set parental controls on devices

   Use parental controls to restrict access to in-app purchases and explicit or exaggerated content, and, on some devices, how long they can spend on the device.

   You’ll likely need to set a password. Make sure it’s different from the password used to access the device, and that your child doesn’t know it.

   Parental controls are usually located under ‘Settings’. See below for more detailed instructions for different devices.

2. Make sure they’re doing school work when they should be

   Try to keep an eye on what they’re up to on devices during school time – make sure they’re actually using them for any work they’ve been set.

   Some virus protection software packages include monitoring features, so check to see if yours has this.

   You can also buy standalone monitoring apps. See this guide for more: https://www.internetmatters.org/resources/monitoring-apps-parents-guide/

3. Talk to your child about staying safe online

   Tell them:

   - ❖ They should only talk to people they know and trust in real life – anyone can pretend to be a child online
   - ❖ If they do talk to people they don’t know, don’t give away personal information – like what street they live on or where they go to school,

or share their location with them. Say no to any requests they get for images or videos, and stop talking to the other person

- Set their profiles to private, to limit what others can see
- Be 'share aware' – think carefully about what they share and with who. Once it's out there, they've got no control over what the other person does with it. Remember, it's illegal to take, share or view sexual images of under-18s, full stop
- If they see something that upsets them, or someone bullies them, tell an adult they trust

Don't feel confident starting a conversation with your child about what they're up to online? Read this advice from the NSPCC: https://www.nspcc.org.uk/keepingchildren-safe/onlinesafety/talking-child-online-safety

4. Agree rules on screen time

There's no recommended 'safe' amount of screen time, but you should try to avoid screens an hour before bedtime.

Agree some limits to stop screen time interfering with your child's sleep or family activities:

- Make a plan together, and stick to it. You could set media-free times and zones, like during meals or in bedrooms
- Model the behaviour you want to see – which may mean no screen time for you at the times agreed with your child. Children are more likely to learn from example
- Try to minimise snacking during screen time
- Turn not using screens into a game, using apps like Forest, where not using devices is rewarded

5. Encourage off-screen activities

Get your child active for the recommended 60 minutes a day:

- See www.nhs.uk/change4life/activities for free ideas for activities and games
- Try an app that's designed to get children active – see the examples at www.internetmatters.org/resources/apps-guide/apps-to-help-kids-getactive/
- Build in screen breaks if they're doing school work at home. 5 to 10 minutes every hour should help. They could take a break to get a drink of water, look out of the window for a few minutes, or do some easy exercises like neck rotations and forward bends

How to set parental controls on your devices

Please note: when following the instructions below, the exact steps you need to take may be a little different depending on the device and software version you're using.

Microsoft devices (Windows computers and Xbox):

You'll need to have a family account set up, with 'child' profiles for your children. Learn more here: https://support.microsoft.com/en-us/help/12413
You can't change existing adult accounts to child accounts.

Set screen time limits

- Go to https://account.microsoft.com/family and sign in to your Microsoft account
- Find your child's name and select 'Screen time'
- Switch 'Use one schedule for all devices' to 'On' to use the same schedule for all devices. Or scroll down and switch on screen time for different devices individually if you want to have separate schedules

You can set time ranges for using devices, and how many hours per day, for each day.

Set age limits for apps, games and media

Online:

- Sign in to your Microsoft account, as above, and find your child's name ⍰ Select 'Content restrictions'
- Go to 'Apps, games and media' and switch 'Block inappropriate apps, games and media' to 'On'. Under 'Allow apps and games rated for', select the age limit you want to apply to your child

On Xbox:

- Sign in with an adult account
- Press the Xbox button on the controller to open the guide, and then select System > Settings > Account > Family
- Select the child account you want to put controls on, select 'Access to content', then select the age limit you want to set

Block inappropriate websites

Online:

- Sign in to your account, find your child's name, and select 'Content restrictions'
- Scroll down to 'Web browsing' and switch 'Block inappropriate websites' to 'On'
- To block specific sites, add links to them under 'Always blocked'
- To make it so your children can only access websites you've explicitly allowed, check the box next to 'Only allow these websites'

Xbox:

- Sign in to an adult account, press the Xbox button and follow the steps to get family settings above
- Select the child account you want to put controls on, then select ‘Web filtering’
- Select the dropdown to see the available options, and choose the level of filtering you want

Manage purchases in the Microsoft Store

Online:

- Sign in to your account, as above, find your child’s name and select ‘Spending’
- Under ‘Ask a parent’, switch ‘Needs adult approval to buy things’ to ‘On’

⍰

Xbox:

- Go into your family settings, as explained above, and choose a child account
- Select Privacy & online safety > Xbox Live privacy > View details & customize > Buy & download and then select ‘On’ in the ‘Ask a parent’ box

Read more here: https://support.microsoft.com/en-us/hub/4294457/microsoftaccounthelp#manage-family

iPads and iPhones:

Set a screen time passcode

- Go to ‘Settings’ (a grey icon with a circular pattern on the home screen) and tap ‘Screen Time’
- Tap ‘Continue’, then choose whether it’s your device or your child’s:
  - If it’s your device and you want to stop your child changing your settings, tap ‘Use Screen Time Passcode’ to create a passcode. Re-enter the passcode to confirm
  - If it’s your child’s device, follow the prompts on the device until you get to ‘Parent Passcode’ and enter a passcode, then re-enter it to confirm

Block in-app purchases

- Go into Settings > Screen Time > Content and Privacy Restrictions. Enter your passcode if asked
- Tap ‘iTunes & App Store Purchases’
- Choose a setting (for example, in-app purchases) and set to ‘Don’t allow’

Block explicit content and set controls on apps

- Go to Settings > Screen Time > Content & Privacy Restrictions > Content Restrictions
- Choose the settings you want for each feature or setting under ‘Allowed Store Content’

Filter website content

This sets restrictions on what websites children can access (e.g. you can limit access to adult content).

- Go to Settings > Screen Time > Content & Privacy Restrictions
- Enter your screen time passcode
- Tap ‘Content Restrictions’, then ‘Web Content’
- Choose ‘Unrestricted Access’ (access to any website), ‘Limit Adult Websites’ (to block access to adult content in Safari) or ‘Allowed Websites Only’ (to set specific websites as ‘approved websites’ and limit access to only these websites)

Read more here: https://support.apple.com/en-gb/HT201304

Fire Tablet

Set a parental controls password

- Swipe down from the top of the screen, then tap ‘Settings’ (a cog icon)
- Tap ‘Parental Controls’
- Tap the switch next to ‘Parental Controls’
- Enter a password, confirm it, then tap ‘Finish’

Restrict apps, features and content

- In ‘Parental Controls’, tap ‘Amazon Content and Apps’ to choose which content or apps you want to block
- You can set your device so that you can only play videos and Twitch (a live streaming platform), and access WiFi and location services, by entering your parental controls password. Go into ‘Password Protection’ in ‘Parental Controls’ to toggle these on
- To block access to Amazon, go to ‘Parental Controls’ and press ‘Amazon Stores (excluding Video)’, and tap to block

Block in-app purchases

- Go to the Amazon Appstore on your device
- Select Account > Settings > Parental Controls
- Tap ‘Enable Parental Controls’, and then enter your account password. Once you’ve done this, your child won’t be able to buy anything in the app without your Amazon password

Restrict available content

- Go Parental Controls > Amazon Content and Apps
- Toggle categories to ‘Blocked’ to block access to relevant apps and games

Set times when your child can use the tablet

- Go to ‘Parental Controls’
- Tap the switch next to ‘Set a Curfew’, then tap ‘Curfew Schedule’
- Set the day and time limits you want

To unlock a device during a curfew, enter your parental controls password.

See here for more information on settings for specific devices, as they can vary:
https://www.amazon.com/gp/help/customer/display.html?nodeId=200127470

Android phones

Set up parental controls

- Open the Play Store app, tap the 3-lines button in the top left > Settings > Parental controls
- Toggle Parental controls to on
- Create a PIN. Make sure to choose a PIN your child doesn't already know

You can then choose the highest age rating you want to allow for apps and games, films, TV, books and music. Go into each option and choose the age rating you want.

Restrict purchases

- Open the Play Store and tap the 3-lines button in the top left
- Select Settings > Require authentication for purchases > For all purchases through Google Play on this device

Manage screen time

You'll need to set up Family Link to do this (see this page for more: https://support.google.com/families/answer/7101025?hl=en) (Family Link is an app that lets parents set "digital ground rules" for their children).

Then, in the Family Link app, select your child and follow the steps below.

To set a daily limit on a device, on the 'Daily limit' card, tap 'Set up' or 'Edit limits' > follow the instructions on the screen.

To set time limits for specific apps (only for devices running Android Nougat or newer), on the 'Today's activity' card, tap 'Set limits' > next to app you want to limit, tap the sand timer icon > Set limit (an icon with the top half of the sand time filled) > set a daily time limit for the app > tap 'Set'.

To set a bedtime, on the 'Bedtime' card, tap 'Edit schedule', then follow the instructions on the screen to set a bedtime.

PlayStation

You'll need to set up accounts for family members, with adult and child accounts, and make sure you and other adults have family manager or parent/guardian status. Read more about how to do this here: https://www.playstation.com/en-gb/get-help/help-library/myaccount/parentalcontrols/family-management/

Set a login passcode and system restriction passcode

A login passcode means that only you can log in to the 'family manager' user on the system.

To do this:

- Go to Settings (this should be shown by a toolbox icon) > Login Settings > Login Passcode Management
- Set a 4-digit passcode using the controller, then re-enter it to confirm

Using a system restriction passcode will prevent your child from changing parental control settings. To do this:

- Go to Settings > Parental Controls/Family Management > PS4 System Restrictions
- Enter the existing system restriction passcode (if you haven't set one before, the default is 0000)
- Select 'Change System Restriction Passcode'
- Enter a new 4-digit passcode using the controller, then re-enter it to confirm

The PlayStation website also explains how to disable new user creation and guest login: https://www.playstation.com/en-gb/get-help/help-library/my-account/parentalcontrols/ps4parental-controls/

Set spending limits

- Go to Settings > Parental Controls/Family Management > Family Management
- Select the user you want to set a spending limit for
- Select 'Applications/Devices/Network Features' under the 'Parental Controls' section ▯ Select 'Monthly Spending Limit' and press X

Restrict access to network features

- Go to Settings > Parental Controls/Family Management > Family Management (you may need to enter your account password)
- Select the user you want to set restrictions for
- Select 'Applications/Devices/Network Features' under the 'Parental Controls' section
- Under 'Network Features', you can choose whether to allow a child user to communicate with other players on the PlayStation Network, or view content created by other players

Set age rating levels for games, Blu-ray Discs and DVDs

- Go to Family Management, as above (you may need to enter your account password) ▯ Select the user you want to set the age level for
- Select 'Applications/Devices/Network Features' and select the content you want to restrict

Sources used in this guide

This factsheet was produced by Safeguarding Training Centre from The Key: www.thekeysupport.com/safeguarding

- Manage devices, apps & screen time, Google for Families Help https://support.google.com/families/topic/7336331?hl=en&ref_topic=6149867
- Should visual display unit (VDU) users be given breaks?, HSE https://www.hse.gov.uk/contact/faqs/vdubreaks.htm
- Guidelines issued on activity and screen time for babies and toddlers, NHS https://www.nhs.uk/news/pregnancy-and-child/who-guidelines-screen-time/
- Physical activity guidelines for children and young people, NHS https://www.nhs.uk/live-well/exercise/physical-activity-guidelines-children-and-youngpeople/
- Share Aware resources for schools and teachers, NSPCC Learning (scroll down to the parent's leaflet in the grey box) https://learning.nspcc.org.uk/researchresources/schools/share-aware-teaching/
- The health impacts of screen time: a guide for clinicians and parents, Royal College of Paediatrics and Child Health https://www.rcpch.ac.uk/resources/health-impactsscreen-time-guide-clinicians-parents
- Sexting in schools and colleges, UK Council for Internet Safety https://www.gov.uk/government/publications/sexting-in-schools-and-colleges