Beechwood Park School

ONLINE SAFETY

AND ACCEPTABLE USE POLICY

Website: www.beechwoodpark.com

Policy Number:	BWPS - 018
Policy Applicable To:	**Whole School – including EYFS**
Policy Revised By:	HM
Last Review Date:	May 2025
SLT Reviewed Date:	May 2025
Governors Reviewed Date:	May 2025
Next Review Date:	May 2026

OVERVIEW:
Beechwood Park recognises the importance of mobile devices and computers for communication and education as well as for recreation and socialising. However, we also recognise that some individuals may use these technologies to harm children. The harm might range from sending hurtful or abusive texts and emails, to grooming and enticing children to engage in sexually harmful conversations, webcam photography or face-to-face meetings. Students may also be distressed or harmed by accessing inappropriate websites that promote unhealthy lifestyles, extremist behaviour and criminal activity. Abuse can take place wholly online and may be used to facilitate offline abuse. Children may also use these technologies in a way that leaves them vulnerable.

AIMS:
Beechwood Park aims to:
- ✓ Ensure secure and supervised access to information and communication technology (ICT) for all pupils
- ✓ Encourage pupils to use technology to support their learning
- ✓ Promote the notion of Digital Health and Safety
- ✓ Encourage all members of the community to gain a healthy balance of ICT use in both school and at home

APPROACH:
Beechwood Park educates pupils about online safety issues across all curriculum subjects, but particularly in the following ways:

- ✓ PSHE lessons
- ✓ Computing lessons
- ✓ Age-specific assemblies

It is essential that children are safeguarded from potentially harmful and inappropriate online material. An effective whole school approach to online safety empowers a school to protect and educate pupils in their use of technology and establishes mechanisms to identify, intervene in, and escalate any concerns where appropriate.

The breadth of issues classified within online safety is considerable and ever evolving, but can be categorised into **four areas of risk:**

- ✓ **Content:** being exposed to illegal, inappropriate, or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, and extremism.
- ✓ **Contact:** being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.
- ✓ **Conduct:** online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g. consensual and non- consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images) and online bullying.
- ✓ **Commerce:** Risks such as online gambling, inappropriate advertising, phishing and or financial scams.

Filters and Monitoring:
The Governing Body does all it can reasonably do to limit children's exposure to the risks described above. The school has safeguarding and filtering systems in place with active monitoring to help create a safe online environment for our pupils. Children are currently not allowed to bring mobile technology into school. Children do not have access to the Wi-Fi code and there is poor 3G/4G/5G currently available on site. A suitable risk assessment for filters has been completed in fulfilling the school's 'Prevent Duty' and the school acknowledges guidance is available from the UK Safer Internet Centre. The Governors are mindful of 'over-blocking' due to filters and monitoring systems. The DSL meets regularly with the IT manager on matters of internet and digital safety, reviewing the effectiveness of filters and monitoring systems.

Education:
The Computing and PSHE schemes of work detail how the school builds resilience in our pupils to protect themselves and their peers through education and information. Our approach to online safety empowers all staff to protect and educate the whole school community in their use of technology and establishes mechanisms to identify, intervene in and escalate any incident where appropriate. Further queries on 'education' should be directed to the Head of Digital Learning and Head of PSHE.

Reporting Internet Safety Concerns:
Any pupil, member of staff or parent who has an internet safety concern should in the first instance refer it to the Designated Safeguarding Lead (DSL), who will take any necessary action in line with the school's Safeguarding Policy. This might include reporting concerns to the police or ESAS.

Where the concerns are not of a safeguarding nature, the issue will be referred to the appropriate pastoral team within the school.

Social networking and other inappropriate sites are blocked and monitored by the school web filtering system to ensure we are compliant with the regulations stipulated in the latest version of KCSIE.

However, the school realises many pupils have access to these sites outside of school. Pupils are reminded that regardless of where their posting originates, any posting of comments, photographs or videos to these sites, YouTube or similar sites which would be derogatory to the school or the school community, or threaten, demean, or bully members of staff or other pupils, is strictly prohibited and may result in disciplinary action being taken by the school.

Overall Responsibilities:
- ✓ Mr. J. Packer is Deputy Head - Pastoral and Designated Safeguarding (and Prevent) Lead for child protection. He will listen and take you seriously if you are concerned about anything to do with online safety, including concerns you may have about another pupil.
- ✓ Mr S. Sadler is our Head of Digital Learning. He will require all pupils to understand the **Acceptable Usage Agreement (Appendix 1)** which they agree to when using Internet connected technology.
- ✓ Mr. D. Williams is our IT Manager and any questions regarding our technical provision/infrastructure should be directed to him. He will work in conjunction with the safeguarding team to review the school filtering and monitoring systems in place to safeguard our pupils.
- ✓ Mrs. A Ridler is our Bursar. She is our Data Protection Co-ordinator who will endeavour to ensure that all personal data is processed in compliance with regulatory requirements

Online Safety and the Prevent Duty:
- ✓ The school delivers a proportionate response with respect to a duty to prevent pupils becoming extremist or radicalised.
- ✓ It is recognised that both encouraging extremism and radicalism is a form of child abuse and all staff must treat suspicions as they would any other form of child abuse.
- ✓ Evidence suggests that social media is the greatest method used by those who wish to encourage extremism and radicalism. The Home Office and DfE have produced a useful paper titled: 'How Social Media Is Used to Encourage Travel to Syria and Iraq'. It can be found here: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/440450/How_social_media_is_u sed_to_encourage_travel_to_Syria_and_Iraq.pdf
- ✓ Additional guidance can be found here: www.saferinternet.org.uk / www.thinkuknow.co.uk

Linked Policies:

This policy should be read in conjunction with the following Beechwood Park policies:

- ✓ Safeguarding and Child Protection Policy
- ✓ Taking, Storing and Using Images of Children Policy
- ✓ Social Media Policy
- ✓ Anti-Bullying Policy
- ✓ Equal Opportunities Policy
- ✓ Pupil Conduct Policy
- ✓ Staff Code of Conduct

Day to Day Responsibilities and Implementation – Beechwood Park's Head of Digital Learning:

- ✓ Writes punctual reports for the Education Committee, updating them on Online Safety developments and ensures that they remain up to date with technological change.
- ✓ Has sole responsibility for ensuring that all staff, pupils, parents and governors have access to and understand this key School policy.
- ✓ Keeps this policy up to date and compliant with law and best practice; Ensures that all staff, pupils, parents and governors understand their responsibility with regards to **Online Safety**.
- ✓ Keeps abreast of current issues and guidance through organisations such as CEOP (Child Exploitation and Online Protection), Childnet, the Hertfordshire Safeguarding Children Partnership, UK Council for Child Internet Safety, Global Kids Online, Digital Futures Commission, Naace, and Better Internet for Kids.
- ✓ Ensures that organisations letting from the school follow all aspects of the BWPS Online Safety Policy and Acceptable Use Agreements.
- ✓ Delivers information and training on Online Safety (Channel and Prevent) to staff in staff meetings, emails, e-Learning and memos.
- ✓ Runs a daily Safeguarding Monitoring Report which monitors all website traffic, alerting the DSL without delay of any concerns.
- ✓ Ensures that all new staff sign the BWPS Acceptable Usage Policy as part of their induction process, recording AUPs with the HR Department.
- ✓ Trains all staff in their individual responsibilities relating to the safeguarding of children in **Online Safety** and ensures that they know what to do in the event of misuse of technology by any member of the school community, including cyberbullying.
- ✓ Provides resources to all staff to incorporate **Online Safety** activities and awareness within their teaching, PSHE and assemblies.
- ✓ Produces regular letters, keeping parents and their children, governors and staff informed of **Online Safety** issues and advice.
- ✓ Advises staff, governors, parents and pupils how to manage screen time safely.
- ✓ Advises staff, governors, parents, and pupils about certification of films and electronic games and posts appropriate **Online Safety** messages in all networked rooms.
- ✓ Finds opportunities to present **Online Safety** messages through email, through assemblies, newsletters and PSHE.
- ✓ Embeds **Online Safety** as a core topic at the start of every year's Digital Learning lessons, finding opportunities when relevant, to discuss **Online Safety** in Digital Learning lessons as the year progresses.
- ✓ Informs staff, governors, parents, and pupils that the school monitors network and internet use.
- ✓ Displays **Online Safety** posters prominently, especially in the IT Rooms.
- ✓ Produces and distributes **Online Safety** (and prevent) posters to be displayed in ancillary areas including all staffrooms, boarding areas, Maintenance and Catering areas and Music Department.
- ✓ Informs the Designated Safeguarding Lead without delay, of any safeguarding concerns.
- ✓ Records that all pupils in Years 3 and above have read and signed the pupil AUP statement annually. Assists the Deputy Head (Academic) and the Deputy Head (Pastoral) with all **Online Safety** investigations.

Beechwood Park's Head of Digital Learning ensures that all pupils understand:

- ✓ The positive and negative impacts of technologies in and out of School or during Remote Learning, on them, their colleagues, parents and beyond and the consequences of negative online behaviour.
- ✓ How to implement copyright etiquette and respect other people's information, images, and the use of Creative Commons licensing.
- ✓ The definition of cyberbullying and the impact of online bullying and how to seek help if they are affected by these issues. How to treat each other's online identities with respect.
- ✓ How to keep control of their digital footprint.
- ✓ How to shape a positive digital identity for themselves.
- ✓ To recognise the difference between their digital rights and their digital responsibilities.
- ✓ How to recognise suspicious, bullying, or extremist behaviour.
- ✓ How to seek advice or help if they experience problems when using the internet and related technologies.
- ✓ How to evaluate materials and learn good searching skills and to be critically aware of the content they access online and guided to validate accuracy of information.
- ✓ How to build practices to help them to adjust their behaviors so as to reduce risks and build resilience.

Managing other Web technologies - The Head of Digital Learning teaches pupils to:

- ✓ Avoid giving out personal details on such sites which may identify them or where they are (full name, address, date of birth, mobile / home phone numbers, photographs, School details, messaging / email address, specific hobbies / interests).
- ✓ Avoid placing images of themselves (or details within images that could give background details) on such sites and to consider the appropriateness of any images they post due to the difficulty of removing an image once online.
- ✓ Use avatars as visual representations of their online personae.
- ✓ Set and maintain profiles on such sites to maximum privacy and deny access to unknown individuals and to Google Search results.
- ✓ Be wary of publishing specific and detailed private thoughts online.
- ✓ Be aware of the role that web browsers and search engines play in tracking their online behaviour.
- ✓ Be discerning in their choices of online tools.
- ✓ Learn how to triangulate the sources of information they discover online in order to verify its veracity.
- ✓ Avoid plagiarising content found on the Internet.
- ✓ Recognise that in school a filter protects them from accessing unsuitable content but at home they need to be more vigilant.
- ✓ Consider carefully anything that is posted online whether through messaging, social media or by other means, only posting messages that they would be happy for a teacher, parents or guardian to see.
- ✓ Avoid viewing, retrieving, downloading or sharing of any offensive material.
- ✓ Never give their personal email address to any website requiring a sign up in school.
- ✓ Never use a personal email address when contacting any adult member of the school community.
- ✓ Not to communicate with staff using social networking sites or other internet-based communication channels.
- ✓ Report any incidents of bullying to the school or incidents whereby pupils have been targeted or influenced to participate in radicalism or extremism to their Form Teacher, Head of Digital Learning or Deputy Head (Pastoral) in line with the BWPS Anti-Bullying Policy.
- ✓ Understand that any device that can or has the potential to be connected to a cellular network or can seamlessly connect to another device using Bluetooth or similar technology (including smartphones), may not be used by a student in School without specific permission being given (until such time as a BYOD policy is implemented).

Beechwood Park's IT Network Manager:

- ✓ Ensures that the school's technological infrastructure is secure and, as far as is possible, is not open to malicious use or attack.
- ✓ Monitors technology uses and practices across the school.
- ✓ Assesses whether any improvements can be made to ensure **online safety.**
- ✓ Ensures that the school has an effective filtering policy in place and is applied and updated regularly.
- ✓ Ensures that the use of the school's technology is regularly monitored and backed up and that any misuse or attempted misuse can be identified by the Head of Digital Learning.
- ✓ Ensures that monitoring software and systems are kept up to date to allow the tracking of the use of email and the internet over the school's network and maintain logs of such usage.

As detailed in the BWPS Anti-Bullying Policy and BWPS Staff Behaviour Policy, staff are reminded that cyberbullying is as unacceptable when carried out by staff members as it is when carried out by pupils.

TERMLY SURVEYS / EVALUATION:

Parental e-Survey: The Head of Digital Learning consults and discusses **Online Safety** with parents / carers annually through an Online Safety Parent Survey.

Michaelmas Term (Pupils):
The Head of Digital Learning oversees the annual Online Safety Pupil Quiz during the Michaelmas Term. Key findings and insights are shared via BeechNET (SharePoint) and Microsoft Teams, with quiz results also accessible to Form Tutors and relevant staff via MS Teams. These outcomes contribute to the ongoing development of the Online Safety Development Plan, aimed at continually enhancing pupils' digital education. The data is also used to inform PSHE sessions, shape future Computing and Citizenship lessons (part of PSHE) as well as support safeguarding reporting. Long term, results will also be made available through a Power BI dashboard on SharePoint.

Lent Term (Staff):
As part of our ongoing commitment to safeguarding and digital literacy, all teaching staff complete an annual Online Safety CPD. The activity encourages staff to consider emerging online risks—such as AI, misinformation, and pupil wellbeing—and supports the continuous development of our Online Safety Development Plan. Insights gathered are shared via HR with the Head of Digital Learning to inform whole-school strategic planning.

Summer Term:
The Head of Digital Learning conducts a comprehensive Online Safety Staff Survey. The results and subsequent recommendations are shared with the Education Committee via MS SharePoint. These are incorporated into the Online Safety Development Plan to ensure a whole-school approach to digital safeguarding.

Password Security
The Head of Digital Learning ensures that all pupils from Year 3 and all staff have individual logins and storage folders on the school network.

The Head of Digital Learning reminds staff and pupils regularly of the need for password security for the internet and ensures all pupils from Year 3 onwards have passwords.

Data Security
Please refer to BWPS Data Protection, Record Keeping and Retention of Records Policy. The Head of Digital Learning reports on data security matters termly at every Education Committee.

Monitoring
The IT Manager agrees the scope of any monitoring of staff communication in writing with both the Headmaster and Bursar. They will consider the following legislation:

- ✓ Data Protection Act 2018 and General Data Protection Regulation (GDPR)
- ✓ The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000,
- ✓ Regulation of Investigatory Powers Act 2000,
- ✓ Human Rights Act 1998 and
- ✓ Keeping Children Safe in Education.

Managing the Internet
The Head of Digital Learning reports on all breaches of the AUP without delay to the Headmaster and Bursar. Where there is a safeguarding concern, the Head of Digital Learning reports the incident without delay to the Designated Safeguarding Lead in accordance with safeguarding policy.

Filters
The School Firewall (WatchGuard) and Web Filter (Smoothwall) control access to the school internet. The filter excludes by category and key words. Use of the web filter considers the age range of pupils, number of pupils, how often they access the IT systems and the proportionality of costs vs. risks.

The Head of Digital Learning and IT Manager

- ✓ Recognise that no filtering system can be 100% effective and that effective online learning practice and supervision support this.
- ✓ Ensure that all staff are aware that they need to preview sites, software, and apps before using them in School or before recommending them to pupils.
- ✓ Ensure that all staff consult with them with details of the site/service before using any online service that requires user accounts to be created or the sharing of any personal data.
- ✓ If teaching staff set internet research for homework, they suggest specific sites ensuring that they have previously checked them.
- ✓ The IT Manager installs anti-virus protection (BitDefender) and keeps it up to date on all School machines, ensuring that the Head of Digital Learning, DSL and SLT Team know of any lapse in protection.

Copyright
The Head of Digital Learning reminds staff frequently of the importance of adhering to copyright legislation. The Head of Digital Learning teaches pupils about copyright and Creative Commons licensing in Computing lessons.

Personal Mobile devices
Please refer to the BWPS Staff Code of Conduct Policy and BWPS Safeguarding and Child Protection Policy. The school is not responsible for the loss, damage or theft of any personal mobile device. Users bringing personal devices into School must ensure that there is no inappropriate or illegal content on the device. A Guest Wi-Fi code is available for adult guests from Reception.

Staff must never use their own mobile devices whilst working with children, except in an emergency. Staff may use mobile personal devices during breaks and only in locations where they cannot be seen or overheard by pupils, parents or visitors.

Under no circumstances may staff use personal mobile phones in, or in the vicinity of the EYFS Department (Woodlands Nursery, Reception)

Publishing Images of Pupils and their Work
Please refer to BWPS Taking, Storing and Using Images of Children Policy

Webcams and CCTV
Staff only use webcams in class for educational purposes. The School operates its CCTV in line with its stated policy.

Misuse and Infringements
- ✓ All staff have a duty to report breaches of this policy to the Head of Digital Learning.

- ✓ The Head of Digital Learning manages all **Online Safety** issues, passing all information available to the Deputy Head (Pastoral) or in the case of safeguarding issues on to the Designated Safeguarding Lead, copying the Bursar and the Headmaster.

- ✓ The Head of Digital Learning logs all **Online Safety** concerns on the Online Safety Concerns File, which the Deputy Head (Pastoral) signs termly.

- ✓ When referred to do so by the Deputy Head (Pastoral), the Head of Digital Learning will provide training for any students who have transgressed in their use of social media.

- ✓ The Head of Digital Learning and Deputy Head (Pastoral) support pupils and staff affected by policy breaches.

- ✓ The Deputy Head (Pastoral) manages all inappropriate or illegal uses of the internet, mobile and digital technologies, under the school's behaviour and disciplinary policies. Breaches may also lead to criminal or civil proceedings.

Equality
Teaching staff take particular care when undertaking internet activities for children with SEN needs, ensuring that such activities are well-planned, well-managed and that they use additional SEN specific resources as appropriate in lessons. Please also refer to BWPS Learning Support Policy.

Parental Partnership
The Head of Digital Learning disseminates information to parents relating to Online Safety where appropriate. The Head of Digital Learning encourages parents/carers to reinforce the guidance from School when using technologies at home.

Appendix 1: BEECHWOOD PARK – PARENT / PUPIL – ACCEPTABLE USAGE AGREEMENT

Dear Parents,

Guidelines for Beechwood Park Pupils Using the School Network, Email and the Internet - Acceptable Usage Agreement (AUA).

We provide guidelines for pupils who are using the school network, email and the internet and the pupils are regularly reminded of their responsibilities when using this system. We would be very grateful if you could read the guidelines below with your child and then sign to agree to the school's acceptable usage policy.

The school will provide a filtered email and internet access service and will record and monitor all use of the system. These guidelines should help you to use the school network, email and the internet safely and responsibly. **Normal school rules for behaviour apply.**

A pupil's use of TEAMS, email and the internet should be guided and controlled in the same way as other information sources, such as television, telephones, films, radios and other potentially offensive media. At school, staff will guide pupils. Outside of school, families bear responsibility for such guidance.

Username and Password:

- ✓ You must never share your passwords or give access to your Beechwood Park systems to anyone else.
- ✓ Use of another person's network account is forbidden.
- ✓ Users must not walk away and leave their computer logged on.

Network:

- ✓ Users should not send or take part in writing any text, or prepare any graphics, or create audio/video material which may be unkind, offensive, abusive, obscene or defamatory; this would be treated as cyber-bullying and is against the law. If you find any material of this nature, you must report it immediately.
- ✓ A user's files are not private. If we think they pose a risk to the system in any way or if any misuse is suspected, these files may be examined and, if necessary, deleted
- ✓ Software programmes or games must not be downloaded, saved to the network or installed.
- ✓ If you need to copy work from your own removable media, please see the Head of Digital Learning/IT Manager.

Email:

- ✓ Whilst at school, you can only use the Beechwood Park email server and your school email address.
- ✓ Whilst you are at school, you may only send emails externally to members of your family and friends whilst boarding whilst under supervision.
- ✓ You are not permitted to send emails to ***any other pupil at Beechwood Park via the Beechwood Park email system,*** either internally or from a computer at home. If you want to contact another pupil, speak to them directly. This is not intended to prevent you from contacting your friends at any time, it's just that email or messaging systems are often not the best way of doing this. Try to communicate face-to-face whenever possible.
- ✓ You must never send an email that contains ***rude, abusive or offensive language***. Emails containing such language are captured and stored. They form part of your record at Beechwood Park.
- ✓ If you receive an email which makes you feel uncomfortable in any way (for example, if it is from someone you don't know or if it contains offensive language or pictures), you must tell a trusted adult immediately. If you are in school, tell a member of staff or go to the Head of Digital Learning for help.

The Internet:

- ✓ Think very hard about the personal information you give out online. If you are being asked to give out personally identifiable information (like your birthday or real name), ask a teacher or a trusted adult before you do so.
- ✓ You should realise the potential dangers of corresponding with unknown people by email or through internet sites. You should never give out details which would enable them to identify and locate you.
- ✓ Do not believe everything you read on the Internet. Even trusted sources can be wrong.
- ✓ Copying and pasting is not good. Do not copy things from websites (or books) unless you have been told to by your teacher. Do not try to claim work, which is not yours, as your own. This is serious and you need to understand this fully before you leave Beechwood Park.
- ✓ You must never attempt to deliberately search for any information that might contain rude, offensive, or abusive, language or pictures.
- ✓ Do not sign up to any chat, email groups or social networking sites (e.g. Facebook, Instagram, Snapchat, Tik Tok etc.) until you are old enough to legally do so. Social media is not allowed at school.
- ✓ Do not request further information from any person, company or organisation using your school email address.
- ✓ Do not use sites that contain chat, chat rooms or forums of any kind.
- ✓ If you find or see a website that makes you feel uncomfortable or scares you, please tell a member of staff.
- ✓ You must not access any games sites during lessons unless a member of staff has asked you to do so.
- ✓ Give yourself a break. Don't stay online too long. Spend time with your friends and family offline.
- ✓ Teach your teachers and parents. Spend time teaching your teachers and parents about your online activities. Show them your favourite websites and explain how you are making good use of the Internet.

Google Classroom and Microsoft Teams:

Whilst engaging with peers and teachers using Microsoft Teams, pupils are reminded to:

- ✓ Adhere to the school's normal expectations on behaviour and appropriate language during the sessions.
- ✓ Report any instance of inappropriate behaviour to a parent / responsible adult and appropriate member of the Senior Leadership Team.
- ✓ Be aware that when working on Microsoft Teams, sessions may be remotely monitored by other members of staff.
- ✓ Only contact teachers using Microsoft Teams or via parents, using school email addresses.
- ✓ Beechwood Park pupils may only use the Chat function within Teams to speak to members of staff not fellow pupils.

Microsoft Teams - Live Audio / Video communication:

In the event of a school closure, we may implement the live audio / video communication functionality of Microsoft Teams. In addition to the above guidance, pupils and parents are informed of the following expectations during any such communication:

- ✓ Pupils must make sure they are dressed appropriately for any audio / video online sessions.
- ✓ Pupils should join virtual sessions from a common area in their house whereby parents and responsible adults can easily supervise sessions.
- ✓ Pupils are not to be in a separate room alone, for example, in their bedroom.

Monitoring:

- ✓ Beechwood Park monitors all internal computer, laptop, tablet and Internet / Network connected device use.
- ✓ Beechwood Park is alerted to content which is deemed inappropriate or where there is a safeguarding concern for the welfare of the pupil.
- ✓ Any concerns logged will be followed up by an appropriate member of staff.

Reporting:

- ✓ If you see something that makes you feel uncomfortable, then please tell a trusted adult as soon as you can. If you're not sure whether the thing you see is illegal, ask the person about it when you tell them.
- ✓ If you are being cyber-bullied or harassed in any way, you should tell a trusted adult as soon as you can. If you are not comfortable telling someone you know, you can contact Childline at http://www.childline.org.uk or by telephone / text at: 0800 111

Sanctions:

- ✓ Any pupil found behaving irresponsibly or inappropriately and not complying with these guidelines will be reported to the appropriate member of staff.
- ✓ Beechwood Park reserves the right to sanction pupils for actions taken outside of school which have an impact on those within. Likewise, pupils will be sanctioned for anything which affects the reputation of Beechwood Park.
- ✓ The school has the right to restrict a pupil's use of the internet / access to connected Internet technology.

Just Remember...

If you are ever in doubt, unsettled by what you see, feel uncomfortable or if you think there is a problem, please ask a trusted adult or member of staff for advice. We will always do our best to help you.

If you are worried about something and you would like to tell someone without talking face-to-face, please message (using Microsoft Teams or via parents, using school email addresses):

- ✓ Mr Sadler – Head of Digital Learning – ssadler@beechwoodpark.com
- ✓ Mr Packer – Deputy Head – DSL – jpacker@beechwoodpark.com
- ✓ Mrs Greenwood / Mrs McIntosh / Mr Darcy – DDSL Team / Heads of School Section

They will get back to you as soon as they can. Please remember that all network, email and Internet usage at Beechwood Park is recorded and monitored.

For further information please contact one of the following members of staff:

- ✓ Mr Sadler – Head of Digital Learning – ssadler@beechwoodpark.com
- ✓ Mr Packer – Deputy Head – DSL – jpacker@beechwoodpark.com
- ✓ Mr Williams – IT Manager – dwilliams@beechwoodpark.com

BEECHWOOD PARK SCHOOL:

Acceptable Use of Information and Communications Technology – Agreement:

Name of Pupil: _____

As the parent or legal guardian of the pupil signing above, I grant permission for my child to use email and the Internet at school. I understand that pupils will be held accountable for their own actions.

I have read through the Guidelines for Beechwood Park Pupils Using The School Network, Email and the Internet with my child. I understand that although access will be through a filtered and monitored service, it may be possible that some of the material accessible may be objectionable.

I accept responsibility for setting standards for my child to follow when using, selecting, sharing and exploring

information and media in line with school expectations, outside the school setting (i.e. at home / on holiday).

Name of Parent: _____ Date: _____

Summary of Recommended Links:

To ensure the BWPS Online Safety Policy remains aligned with current statutory and best practice guidance, we have included the following references and resources which staff should also review:

DfE – Generative AI in Education (2023)

This official government guidance outlines how BWPS can approach the safe and responsible use of Generative Artificial Intelligence (AI) tools. We will look to future-proof our policy as new technologies emerge, demonstrating our commitment to staying aligned with the Department for Education's latest advice.

*Generative AI in Education LINK

DfE – Keeping Children Safe in Education (KCSIE)

The statutory KCSIE guidance places a strong emphasis on online safety as a core safeguarding issue. It requires schools to implement appropriate filtering and monitoring systems, which we currently have in place.

*KCSIE and Online Safety LINK

DfE – Data Protection in Schools (2025)

Please note the link to the DfE's toolkit on data protection which highlights BWPS's commitment to upholding UK GDPR standards—especially in relation to student data and online activity logs.

*View the toolkit LINK

UK Safer Internet Centre / SWGfL Resources

Incorporating links to resources from the UK Safer Internet Centre and SWGfL (such as their policy templates and the 360° Safe self-review tool) demonstrates that BWPS look to be benchmarked against nationally recognised best practices.

*UK Safer Internet Centre and SWGfL LINK

Prevent Duty Guidance

The Prevent Duty (under the Counter-Terrorism and Security Act 2015) requires schools to protect students from radicalising content online. Our policy reflects our statutory obligation to monitor and filter for extremist materials and educate pupils about associated online risks.

*Prevent Duty Link