Online Safety Policy

Author – Gareth Allen – Executive Headteacher

Created: April 2026

Review date: April 2027

Part of esteem emat Multi-Academy Trust

TABLE OF CONTENTS

Aims

Bracken Hill School is committed to ensuring a safe, supportive and inclusive digital environment for all pupils, staff and members of the wider school community. We recognise that online safety is an integral part of safeguarding and wellbeing, and that pupils with special educational needs and disabilities (SEND) may be disproportionately vulnerable to online harm.

This policy aims to:

- Ensure robust safeguarding arrangements are in place to protect pupils and staff from online risks, including those associated with emerging technologies such as artificial intelligence (AI)
- Provide a preventative, proportionate and inclusive approach to online safety that reflects the needs of a specialist school community
- Clearly define roles, responsibilities and accountability in relation to online safety, filtering and monitoring
- Support pupils to develop appropriate digital literacy, communication and resilience skills, taking account of cognitive ability, communication need and individual vulnerability
- Ensure effective filtering and monitoring systems are in place on all school-owned devices and networks, in line with Department for Education expectations
- Establish clear procedures for identifying, reporting, responding to and recording online safety concerns and safeguarding incidents

The four key categories of online risk

Our approach to online safety is structured around the four categories identified in national guidance, interpreted through a SEND and vulnerability-aware lens:

Content: Exposure to illegal, inappropriate or harmful material, including (but not limited to): pornography; violence; extremist content; disinformation and misinformation; misogyny; self-harm and suicide content; hate speech; and AI-generated or manipulated content (including deepfakes).

Contact Harmful online interaction, including grooming, coercion, peer-on-peer abuse, exploitation, online persuasion, or inappropriate contact from adults or other young people.

Conduct Online behaviours that may cause harm, including bullying, harassment, abusive communication, misuse of technology, creation or sharing of images without consent (including AI-generated imagery), and difficulties understanding social boundaries in online communication.

Commerce Online risks such as scams, phishing, financial exploitation, in-app purchases, gambling, advertising manipulation and data harvesting.

Contextual safeguarding and SEND

The school recognises that:

- pupils with SEND may have reduced capacity to assess risk
- some pupils may take online content literally
- communication tools may form a core part of identity, autonomy and access

Online safety education, supervision, filtering and responses will therefore be adapted, individualised and proportionate, in line with pupils' cognitive, communication and emotional needs.

Legislation and guidance

This policy is informed by, and should be read alongside, the following statutory and non-statutory guidance:

- **Keeping Children Safe in Education (KCSIE)** – *September 2025*, and in anticipation of expectations within the draft 2026 update, particularly in relation to:
  - filtering and monitoring governance
  - artificial intelligence and emerging online risks
  - safeguarding vulnerability and contextual harm
- **Working Together to Safeguard Children** – statutory inter-agency safeguarding guidance
- **Teaching Online Safety in Schools** (DfE)
- **DfE Digital and Technology Standards**, including:
  - Filtering and Monitoring Standards for Schools and Colleges
  - Cyber Security Standards
- **Searching, Screening and Confiscation** (DfE)
- **Prevent duty guidance: Guidance for specified authorities in England and Wales** – protecting pupils from radicalisation and extremism
- **Data protection: The UK's data protection legislation - GOV.UK**
- **Education Act 1996**, **Education and Inspections Act 2006**, **Education Act 2011**
- **Equality Act 2010**, with particular regard to disability and reasonable adjustments

Where guidance is updated during the lifetime of this policy, the school will respond proportionately and revise practice as required.

Artificial Intelligence (AI) and Emerging Technology

This policy reflects the Department for Education's published guidance on the safe and effective use of AI in education and recognises that:

- AI presents significant safeguarding, data protection and wellbeing considerations

- risks include misinformation, hallucinations, synthetic or manipulated content, and misuse for exploitation or bullying
- staff and pupil use of AI must be risk-assessed, clearly bounded and aligned with safeguarding expectations

AI is therefore addressed explicitly within this policy as an online safety and safeguarding issue, not solely a curriculum matter.

Personal devices, AAC & specialist access devices and medical need

Bracken Hill School does not operate a general Bring Your Own Device (BYOD) model for pupils.

The only permitted exceptions are the use of approved Augmentative and Alternative Communication (AAC) devices, specialist access technology, or devices required for medical purposes, where:

- the device is essential to support communication, learning, access or an identified medical need
- its use is expressly agreed and documented as part of a personalised plan or medical arrangement
- use is purpose-specific and limited to the agreed function
- appropriate supervision, safeguarding measures, filtering and monitoring controls are in place
- use complies with this policy, Acceptable Use Agreements and wider safeguarding arrangements

Approved AAC, specialist access and medical devices are recognised as assistive or health-support tools, not discretionary personal technology, and their use is managed accordingly.

Roles and responsibilities

Online safety is recognised as a shared safeguarding responsibility. Clear leadership, accountability and understanding of roles are essential to ensure that pupils are protected effectively, particularly in a specialist context where vulnerability, communication need and cognitive profile may increase risk.

All members of the school community must act in accordance with this policy and related safeguarding procedures.

The Governing Board

The governing board has strategic oversight of online safety and holds senior leaders to account for the effective implementation of this policy.
In fulfilling this responsibility, the governing board will:

- ensure that this Online Safety Policy is reviewed at least annually and in response to changes in statutory guidance

- ensure that appropriate filtering and monitoring systems are in place on all school-owned devices and networks
- receive assurance from senior leaders that filtering and monitoring arrangements are effective, proportionate and reviewed regularly
- ensure that online safety, including filtering and monitoring, forms part of the school's wider safeguarding framework
- ensure that all staff receive appropriate safeguarding and online safety training, including understanding their role in filtering and monitoring
- ensure that online safety provision and teaching is appropriate to pupils with SEND and additional vulnerabilities

The governing board does not manage day-to-day online safety arrangements but expects clear reporting and accountability from senior leaders and the Designated Safeguarding Lead.

The Safeguarding link governor will have oversight of safeguarding and online safety.

The Executive Headteacher / Head of School

The Executive Headteacher and Head of School have overall responsibility for ensuring the safety and wellbeing of pupils and staff, including online safety.

They will:

- ensure that this policy is implemented consistently across the school
- ensure that online safety is embedded within safeguarding culture, policies and staff practice
- ensure clear delegation of operational responsibility to the Designated Safeguarding Lead (DSL)
- ensure that staff are trained, supported and confident in responding to online safety concerns
- ensure that systems, staffing and resources are sufficient to meet filtering, monitoring and safeguarding expectations
- ensure that serious online safety concerns involving staff are managed in line with safeguarding and allegations procedures

The Designated Safeguarding Lead (DSL)

The Designated Safeguarding Lead (DSL) takes lead responsibility for online safety as part of their safeguarding role.

This includes ownership and understanding of filtering and monitoring arrangements, in line with statutory guidance.

The DSL will:

- take strategic and operational responsibility for online safety within the school
- ensure that online safety concerns are managed in line with child protection procedures

- understand how the school's filtering and monitoring systems work, what they do and do not cover, and their safeguarding limitations
- ensure that safeguarding alerts arising from monitoring systems are responded to promptly and appropriately
- work closely with technical staff to ensure filtering and monitoring arrangements remain effective and proportionate
- provide assurance to the governing board regarding the effectiveness of filtering and monitoring systems
- ensure that online safety incidents are appropriately recorded and reviewed
- ensure that emerging risks, including those associated with artificial intelligence, manipulated content and online exploitation, are reflected in practice and training
- ensure online safety approaches take account of SEND, communication needs and individual vulnerability
- deliver or coordinate staff training and updates relating to online safety
- liaise with external agencies where necessary, including safeguarding partners, the local authority or the police

IT Lead

The Trust's ICT Lead is responsible for the technical implementation of online safety measures and works under the strategic direction of senior leaders and the DSL.

They will:

- install, manage and maintain filtering and monitoring systems on school-owned devices and networks
- ensure that illegal and inappropriate content is blocked in accordance with statutory expectations
- ensure that filtering and monitoring systems are reviewed and tested regularly
- maintain secure network infrastructure, including access controls and device management
- keep appropriate records relating to technical incidents or changes
- implement agreed configurations for approved AAC or specialist devices, where these require network access
- ensure that attempts to bypass filtering or security controls are identified and reported

The IT lead does not determine safeguarding thresholds or responses – these remain the responsibility of the DSL.

All Staff and Volunteers

All staff and volunteers have a responsibility to:

- read, understand and follow this Online Safety Policy
- adhere to the Staff Acceptable Use Agreement
- uphold safeguarding responsibilities at all times
- remain vigilant to online safety concerns, including those arising from pupil communication, behaviour or distress

- understand their role in filtering and monitoring, including:
  - what to do if they believe filtering has failed
  - how to report concerns promptly
- supervise pupils appropriately when technology is being used
- ensure that any online safety concerns are reported to the DSL without delay
- model safe, professional and appropriate digital behaviour
- follow clear boundaries around technology use, including personal devices

Staff must not use unapproved digital tools, platforms or AI systems with pupils.

Pupils

Pupils are supported and expected, at a level appropriate to their age, ability and needs, to:

- use technology safely, respectfully and as directed by staff
- understand basic rules for online safety and digital behaviour
- communicate using technology in ways that are appropriate and safe
- report concerns or worries about online content or contact to a trusted adult

Expectations for pupils are personalised to reflect SEND, communication needs and supervision levels.

Parents and Carers

Parents and carers are expected to:

- support the school's approach to online safety
- engage with guidance shared by the school
- reinforce safe online behaviours at home where appropriate
- raise concerns about online safety promptly with school staff

The school recognises that parents and carers may require additional support and guidance due to the complexity of online risks and the needs of pupils with SEND.

Visitors and External Professionals

Visitors and external professionals using school systems or devices must:

- comply with this policy and Acceptable Use expectations
- use school technology only for professional purposes
- report any online safety concerns to a member of staff

Specific clarification: Personal devices and AAC

Staff and pupils are not permitted to bring or use personal devices (Bring Your Own Device – BYOD) within school.

The only exception to this is the use of approved Augmentative and Alternative Communication (AAC) or specialist access devices, where such devices are required to support communication, learning or access needs.

Any permitted AAC or specialist device use must be:

- explicitly agreed by the school

- subject to appropriate safeguarding controls and supervision
- consistent with filtering, monitoring and acceptable use arrangements

AAC and specialist access devices are treated as assistive communication tools, not discretionary personal technology.

Educating pupils about online safety

Bracken Hill School recognises that educating pupils about online safety is a core safeguarding responsibility. Teaching is designed to help pupils develop the knowledge, understanding and skills needed to engage safely with digital technology, within the limits of their developmental, cognitive and communication needs.

Online safety education is delivered in a way that is:

- developmentally appropriate
- individualised
- carefully scaffolded
- reinforced through adult supervision and modelling

We do not assume that pupils will develop full independence online; instead, education focuses on supported and safe engagement, recognising that adult responsibility remains central.

Curriculum approach

Online safety education is embedded within:

- Computing
- PSHE / Relationships and Health Education
- communication and life-skills programmes
- therapeutic and pastoral work
- daily classroom practice and routines

Key messages are revisited regularly and reinforced through:

- visual supports
- repetition and consistency
- modelling by trusted adults
- adapted language and symbols
- targeted interventions where needed

Teaching is always adapted to reflect pupils':

- SEND profiles
- communication needs
- emotional regulation needs
- trauma history or vulnerability

Core themes of online safety education

Pupils are supported, at an appropriate level, to develop understanding of the following areas:

Safe use of technology

- using devices only with adult permission
- understanding that devices and online spaces are supervised
- recognising that technology is a tool for learning and communication, not unrestricted access

Communication and relationships

- understanding appropriate and inappropriate communication
- recognising unsafe requests or messages
- developing an understanding of consent and boundaries (where appropriate)
- recognising that people may not be who they claim to be online

Keeping personal information safe

- learning what personal information is
- understanding the importance of privacy
- knowing that personal information should not be shared without adult support

Recognising harm and seeking help

- identifying content that is frightening, upsetting or confusing
- knowing how to signal distress or concern
- knowing which adults are safe to talk to
- understanding that asking for help is always the right thing to do

Adaptation for individual need

Where necessary:

- online safety education is personalised through EHCP outcomes
- additional support or intervention is provided
- communication strategies are adapted for AAC users
- teaching is delivered in smaller groups or 1:1 contexts

This ensures that online safety education remains meaningful, accessible and protective, rather than abstract or overwhelming.

Artificial intelligence, misinformation and manipulated content

The school recognises that artificial intelligence (AI) is increasingly present in digital content and may pose particular risks for pupils with SEND.

Where appropriate, pupils are supported to understand that:

- some online content (images, videos or messages) may be fake or manipulated
- AI can create images, audio or video that look real but are not
- online information may not always be true or reliable
- technology should not be trusted without adult support and checking

Education around AI and misinformation focuses on:

- simple, concrete explanations
- critical awareness at an accessible level
- reinforcing the role of adults in helping pupils interpret information safely

Safeguarding by design

Online safety education at Bracken Hill School is underpinned by the principle of safeguarding by design, meaning that:

- pupils are not expected to manage risks independently
- access to technology is planned, supervised and controlled
- filtering, monitoring and adult presence sit alongside education
- communication tools (including AAC) are treated as support mechanisms, not open platforms

This approach recognises that education alone is not sufficient protection for pupils who may be vulnerable or have limited risk awareness.

Educating parents and carers about online safety

Bracken Hill School recognises that parents and carers play an important role in supporting children and young people to be safe online. We also recognise that families of pupils with SEND may face additional challenges, particularly where pupils have:

- communication difficulties
- limited understanding of risk
- high levels of anxiety
- strong reliance on digital communication tools
- restricted independence

The school therefore takes a supportive, partnership-based approach, rather than assuming parental oversight alone is sufficient.

Communication and information sharing

The school will seek to inform and support parents and carers by:

- sharing this Online Safety Policy via the school website and on request
- providing information through newsletters, letters and other routine communications
- incorporating online safety information into parent and carer meetings where appropriate
- signposting trusted external guidance and resources
- responding promptly and sensitively to concerns raised by families

Information shared with families is designed to be clear, proportionate and accessible, avoiding unnecessary technical language.

Understanding school systems and expectations

Parents and carers will be informed about:

- how technology is used in school
- the school's filtering and monitoring arrangements
- the fact that the school does not permit Bring Your Own Device (BYOD) for pupils or staff, except for approved AAC or specialist access devices
- how AAC or specialist devices are supported, supervised and safeguarded

The school will be transparent about how online safety is managed in practice, while maintaining appropriate confidentiality and security.

Shared safeguarding responsibility

While parents and carers retain responsibility for managing online activity outside school, Bracken Hill School recognises that this responsibility must be viewed in context.

The school will:

- avoid unrealistic expectations of parental control
- recognise that many pupils require ongoing adult supervision online
- offer guidance that reflects pupils' developmental and communication needs
- work collaboratively with families where risks or concerns are identified

Parents and carers are encouraged to inform the school of any online safety concerns that may affect a pupil's wellbeing, even if the activity occurs outside school.

Responding to concerns

Parents and carers should raise online safety concerns by contacting:

- the class team
- a member of the safeguarding team
- or the Designated Safeguarding Lead (DSL)

The school will:

- listen carefully to concerns
- assess risk in line with safeguarding procedures
- take appropriate action where concerns impact on a pupil's safety, wellbeing or access to education
- work with families and external agencies where necessary

Building consistency for pupils

For many pupils with SEND, consistent messages across home and school are essential.

Where appropriate, the school will work with parents and carers to:

- reinforce key safety messages
- agree shared boundaries or expectations
- support pupils who struggle to recognise risk or regulate online behaviour
- ensure that AAC or communication technology is used safely and purposefully

Cyber-bullying and harmful online behaviour

Bracken Hill School recognises that bullying and harmful behaviour can occur through digital technologies and online communication, and that pupils with SEND may be particularly vulnerable due to difficulties with communication, social understanding, emotional regulation or recognising risk.

Cyber-bullying and online peer harm are treated as safeguarding concerns, not simply behaviour issues.

Online harm may take place:

- during the school day
- using school systems
- outside school hours, where it impacts on a pupil's wellbeing, safety or ability to access education

All incidents will be responded to in line with the school's safeguarding and behaviour policies, with a protective and proportionate approach.

Definition

Cyber-bullying refers to bullying or harmful behaviour that takes place using digital technology. This may include, but is not limited to:

- abusive or threatening messages
- repeated unwanted contact
- impersonation or identity misuse
- sharing images, videos or messages without consent
- humiliation, coercion or control through online communication
- exclusion from digital spaces

In a SEND context, harm may occur even where intent is unclear. Behaviour that causes distress, fear or emotional harm will be taken seriously regardless of motivation or understanding.

SEND-informed understanding of harm

The school recognises that:

- some pupils may not recognise that their behaviour is harmful
- some pupils may be easily influenced, coerced or exploited
- online communication may feel more intense or confusing than face-to-face interaction
- pupils may comply with requests without understanding risk

As a result, responses to cyber-bullying focus on:

- safeguarding and protection first
- education and support
- proportionate behaviour management where appropriate

Prevention and education

The school seeks to prevent cyber-bullying and online peer harm through:

- supervised and structured use of technology
- clear boundaries around digital communication
- adapted online safety education (see Section 4)
- modelling respectful communication by adults
- consistent messages reinforced across the curriculum and pastoral support

Pupils are supported to:

- recognise when something feels unsafe or upsetting
- understand that they can say no

- seek help from trusted adults
- understand that reporting concerns will not result in punishment

Artificial intelligence and emerging forms of harm

The school recognises that AI can be misused to cause harm, including through:

- impersonation
- fake messages or images
- manipulated or “deepfake” content
- humiliation or coercion

Any use of AI-generated content to intimidate, embarrass, threaten or harm others will be treated as a serious safeguarding concern and managed in line with this policy and safeguarding procedures.

Responding to cyber-bullying and online harm

All incidents of suspected cyber-bullying or online peer harm will be:

- taken seriously
- recorded appropriately
- investigated proportionately
- responded to in line with safeguarding procedures

Responses may include:

- immediate safeguarding action
- pastoral or therapeutic support
- review of access to technology
- work with parents and carers
- involvement of external agencies where necessary

Where behaviour may be harmful but arises from SEND-related need, responses will prioritise support, education and protection, rather than punishment.

Searching and examination of devices

The school has the power to search for and examine electronic devices where there is reasonable cause to believe that:

- a pupil is at risk of harm
- a safeguarding concern has occurred
- school rules have been breached

Any searching, screening or deletion of content will be carried out:

- in line with statutory guidance
- proportionately
- with safeguarding considerations at the centre

If there is reason to believe a device contains indecent images of a child, staff will:

- not view the content
- secure the device
- report immediately to the Designated Safeguarding Lead

Reporting and support

Pupils, staff and parents/carers are encouraged to report concerns as early as possible.

Concerns should be reported to:

- a trusted adult
- the safeguarding team
- or the Designated Safeguarding Lead (DSL)

The school will ensure that:

- pupils feel safe to disclose concerns
- responses are calm, supportive and protective
- safeguarding decisions are clearly recorded

Acceptable use of the internet in school

Bracken Hill School provides access to the internet and digital technologies to support learning, communication and wellbeing. All use of the school's internet and digital systems is subject to this policy and the relevant Acceptable Use Agreements.

Use of the internet in school is a privilege, not a right, and is closely supervised in order to safeguard pupils and staff.

School-owned devices and systems

All internet access in school takes place through:

- school-owned devices
- school-managed networks
- school-approved software, platforms and services

Staff and pupils are not permitted to access the school network using personal devices (Bring Your Own Device – BYOD), with the sole exception of approved AAC or specialist access devices, as set out elsewhere in this policy.

Purpose of internet use

The school's internet access must only be used:

- for educational purposes
- for authorised communication
- for professional duties linked to a staff member's role

Use of the internet for personal, recreational or non-educational purposes is not permitted during the school day unless explicitly authorised.

Supervision and safeguarding

Internet use by pupils will always be:

- planned
- supervised
- appropriate to individual need

The school does not assume that pupils are able to self-regulate online activity safely. Adult supervision and professional judgement are central safeguards.

Where pupils use communication technology (including AAC), this is supported and monitored as part of a structured learning or communication programme.

Filtering, monitoring and oversight

All internet use on school systems is subject to filtering and monitoring in line with statutory expectations.

This includes:

- blocking access to illegal, harmful or inappropriate content
- monitoring activity to identify safeguarding concerns
- reviewing alerts or concerns promptly

Staff and pupils should be aware that privacy cannot be assumed when using school systems, as safeguarding monitoring is in place.

Attempts to bypass filtering, monitoring or security controls are not permitted and will be treated as a safeguarding and disciplinary matter.

Expectations for staff

Staff must:

- follow the Staff Acceptable Use Agreement
- use only approved digital tools and platforms
- model safe, professional online behaviour
- ensure pupils use technology safely and appropriately
- report any concerns about internet use immediately to the DSL

Staff must not:

- use unapproved websites, platforms or AI tools with pupils
- allow pupils to access inappropriate content, even inadvertently
- permit unsupervised internet access

Expectations for pupils

Pupils are supported, according to their age and ability, to:

- use the internet only with adult permission
- follow clear routines and expectations for technology use
- stop and seek help if something feels unsafe, upsetting or confusing

Expectations for pupils are personalised and adjusted in line with SEND needs and communication profiles.

Breaches of acceptable use

Any breach of acceptable internet use will be:

- responded to proportionately
- managed in line with safeguarding and behaviour procedures

- recorded where appropriate

Where internet misuse indicates safeguarding risk, child protection procedures will take precedence over behaviour sanctions.

Pupils using mobile devices in school

Bracken Hill School recognises that some pupils may bring personal mobile phones to school for reasons linked to travel, safety or transition. However, stringent controls are in place to ensure that mobile devices do not present a safeguarding risk.

The school does not permit the use of personal mobile devices on site, except where explicitly stated below.

Mobile phones brought to school

Pupils attending provision on the Bracken Hill School site, may bring a personal mobile phone to school, but:

- the phone must be handed in immediately on arrival
- the phone is stored securely by the school during the school day
- the phone is returned to the pupil only at the end of the school day
- the phone must not be accessed or used on site

Pupils are not permitted to use their mobile phones:

- in lessons
- during breaks or social times
- during transitions
- or anywhere on the school site

Any failure to hand in a phone, or any attempt to use a personal mobile device on site, will be treated as a breach of school rules and managed in line with behaviour and safeguarding procedures.

Exception: Approved AAC and Specialist Access Devices

The only exception to the above arrangements is the use of approved Augmentative and Alternative Communication (AAC) or specialist access devices, where such devices are essential to support a pupil's communication, learning or access needs.

Where AAC or specialist access devices are permitted:

- use is explicitly authorised by the school and documented as part of an agreed plan
- use is planned, supervised and limited to the specified purpose
- appropriate safeguarding, filtering and monitoring controls are applied
- expectations and arrangements are shared with parents and carers

Approved AAC and specialist access devices are treated as assistive communication tools, not personal mobile phones. Their use does not permit unrestricted access to the internet, messaging or other digital services beyond the agreed function.

Safeguarding and supervision

The school does not expect pupils to self-regulate the safe use of mobile technology. Adult oversight remains the primary safeguarding measure.

Any concerns relating to mobile device use will be:

- addressed promptly
- assessed in line with safeguarding procedures
- recorded where appropriate

Where mobile phone use indicates potential safeguarding risk, child protection procedures will take precedence over behaviour sanctions.

Staff using work devices outside school

Bracken Hill School recognises that staff may, at times, need to use school-owned devices outside the school site in order to carry out their professional duties. This may include preparation, assessment, planning, record-keeping or approved remote working.

All use of school devices outside school must be secure, professional and safeguarding-aware.

Approved devices and access

When working outside school, staff are expected to use school-owned devices for the majority of school business, particularly where this involves pupil data, safeguarding information or confidential records.

However, the school recognises that staff may access limited systems, such as school email or calendar services, on personal mobile devices where this has been approved.

Where personal mobile devices are used in this way:

- access is restricted to low-risk systems only (e.g. email)
- two-step / multi-factor authentication must be enabled and used at all times
- no pupil or safeguarding data may be downloaded, stored or transferred to the personal device
- devices must be protected by a secure passcode or biometric lock
- lost or compromised devices must be reported immediately

Staff are not permitted to use personal devices to:

- access or record safeguarding systems
- store pupil data or sensitive information
- complete assessment, reporting or record-keeping tasks
- communicate with pupils outside approved systems

Any access to school systems via personal devices remains subject to monitoring and safeguarding oversight.

Security and data protection

Staff using work devices outside school must take all reasonable steps to ensure device and data security, including:

- keeping devices password-protected at all times
- ensuring devices lock automatically when not in use
- not sharing devices with family members or others
- not allowing unauthorised access to school systems
- ensuring data is stored only on approved school systems

If a device is lost, stolen or believed to be compromised, staff must inform the school immediately, in line with data protection and safeguarding procedures.

Use of removable media and cloud services

Staff must not:

- download pupil or staff data onto personal storage devices
- use unapproved cloud-based services
- transfer data via personal email accounts

Any use of removable media or cloud services must be:

- explicitly approved
- encrypted where required
- compliant with data protection requirements

Use of artificial intelligence (AI) by staff

Bracken Hill School recognises that artificial intelligence (AI) tools are increasingly available and, when used appropriately, may support efficiency, accessibility and professional practice.

The school permits the use of specific, approved AI tools for professional purposes, subject to clear safeguarding and data protection boundaries.

Approved AI tools

Microsoft Copilot for Microsoft 365

Staff have access to Microsoft Copilot for Microsoft 365 as part of the school's secure Microsoft 365 tenancy. Copilot 365 operates within the organisation's controlled environment and is subject to:

- organisational security controls
- user authentication
- audit logging
- data protection and retention policies

As such, Microsoft Copilot 365 is considered an approved AI tool when used in line with this policy.

Staff may use Copilot 365 to support professional and administrative tasks such as:

- drafting, refining or summarising documents
- planning and preparation
- improving clarity or accessibility of written material
- routine administrative efficiency

All outputs remain subject to professional checking and judgement.

Safeguarding and professional boundaries

When using any AI tool, staff must:

- **never rely on AI to make safeguarding decisions**
- never use AI tools directly with or alongside pupils
- ensure AI supports, but does not replace, professional judgement
- apply the same standards of confidentiality and professionalism as with any other digital tool

AI must not be used as a substitute for:

- safeguarding thresholds
- assessment of risk
- decision-making about pupil safety or wellbeing

Unapproved AI tools

Staff must not use:

- public or consumer AI platforms
- personal AI accounts
- AI tools outside those explicitly approved above

for any school business involving:

- pupils
- safeguarding matters
- personal or sensitive information
- professional decision-making

Professional accountability

All use of AI is subject to:

- professional standards
- monitoring and audit
- safeguarding and disciplinary procedures

Staff remain fully accountable for any content produced or decisions made when using AI tools.

Professional conduct and safeguarding

When using work devices outside school, staff must:

- maintain professional standards at all times
- ensure all communication remains appropriate and authorised
- use only approved platforms for school communication
- uphold clear boundaries with pupils and families

Staff must be aware that all school devices and systems may be subject to monitoring and audit.

Breaches and concerns

Any misuse of school devices, whether inside or outside school, may:

- be treated as a disciplinary matter
- raise safeguarding concerns
- require reporting under data protection procedures

Where concerns relate to safeguarding, child protection procedures will take precedence.

How the school will respond to issues of misuse

Bracken Hill School recognises that misuse of digital technology may involve safeguarding concerns, behavioural issues, or both. The school's response will always prioritise safeguarding and protection, particularly where pupils with SEND may be vulnerable or unable to recognise risk.

All incidents will be managed proportionately, recorded appropriately and reviewed to inform future practice.

Principles guiding the school's response

When responding to issues of misuse, the school will:

- take a calm, considered and proportionate approach
- prioritise the safety and wellbeing of pupils
- recognise the impact of SEND, communication needs and cognitive understanding
- distinguish between:
    - accidental exposure
    - lack of understanding
    - intentional misuse
    - coercion, exploitation or peer harm
- ensure responses are educational and supportive where appropriate, and protective where risk is identified

Behaviour sanctions will never replace safeguarding action where there are child protection concerns.

Responding to pupil misuse

Where a pupil misuses the school's internet, devices or digital systems, the response may include:

- immediate safeguarding assessment
- removal or restriction of access to technology
- pastoral or therapeutic support
- restorative or educational interventions
- involvement of parents or carers
- referral to external agencies where required

The response will take account of:

- the nature and seriousness of the incident
- the pupil's SEND profile and capacity
- whether harm has occurred or risk is ongoing

All responses will be consistent with the school's safeguarding and behaviour policies.

Responding to safeguarding concerns

If an incident involves or indicates:

- exposure to harmful or illegal content
- exploitation, grooming or coercion
- peer-on-peer abuse
- threats to a pupil's safety or wellbeing

the matter will be treated as a safeguarding concern and managed in line with child protection procedures.

The Designated Safeguarding Lead (DSL) will:

- assess risk
- determine next steps
- liaise with external agencies where appropriate
- ensure actions and decisions are recorded clearly

Responding to staff misuse

Where a member of staff is suspected of misusing digital technology, school systems or online tools, the matter will be addressed in line with:

- the Staff Code of Conduct
- disciplinary procedures
- safeguarding and allegations management procedures

If concerns relate to safeguarding or professional boundaries, the DSL and senior leaders will take immediate action in line with statutory guidance.

Illegal or high-risk activity

If there is reason to believe that digital misuse involves illegal activity, including but not limited to:

- indecent images of children
- serious exploitation or grooming
- extremist material

the school will:

- not investigate independently
- preserve evidence as appropriate
- take advice from the DSL
- refer to the police or relevant authorities without delay

Staff must never view or share illegal material.

Recording and review

All significant incidents of misuse will be:

- logged appropriately
- reviewed by safeguarding leaders
- monitored for patterns or repeat concerns
- used to inform training, supervision or policy review

This ensures that online safety practice remains responsive and continually improving.

Training for staff, governors and volunteers

Bracken Hill School recognises that effective online safety depends on staff, governors and volunteers having the knowledge, confidence and professional judgement to identify concerns and respond appropriately.

Online safety training is treated as a core component of safeguarding training.

Staff training

All staff, including teachers, support staff and peripatetic staff, will:

- receive online safety training as part of safeguarding induction
- receive regular safeguarding updates that include online safety
- be made aware of:
    - emerging online risks, including AI-enabled harm
    - Child-on-Child online abuse
    - exploitation, coercion and grooming
    - filtering and monitoring expectations
    - staff responsibilities when using digital systems

Training is adapted to reflect:

- the SEND context of the school
- communication and cognitive needs of pupils
- the balance between support, supervision and protection

Staff will be trained to understand their role in filtering and monitoring, including:

- recognising when systems may not be effective
- responding to safeguarding alerts appropriately
- reporting concerns promptly to the Designated Safeguarding Lead (DSL)

Designated Safeguarding Lead (DSL) and safeguarding leads

The DSL and any deputies will:

- receive specialist safeguarding training at least every two years
- undertake regular updates and professional development
- maintain a secure understanding of:
    - filtering and monitoring systems
    - online safeguarding risks
    - AI and emerging digital harms

- statutory guidance and local safeguarding arrangements

This ensures the DSL is able to provide informed leadership, challenge and assurance.

Governors

Governors will receive safeguarding training appropriate to their role, which includes:

- online safety as part of safeguarding oversight
- understanding of filtering and monitoring responsibilities
- awareness of emerging risks and statutory expectations
- assurance roles rather than operational involvement

Training enables governors to:

- ask informed questions
- challenge practice appropriately
- hold leaders to account for implementation of this policy

Volunteers and external professionals

Volunteers and external professionals working with pupils will:

- receive appropriate online safety information as part of induction
- be made aware of this policy and acceptable use expectations
- understand how to report concerns to school staff or the DSL

Training will be proportionate to role and level of contact with pupils.

Monitoring and review of training

The school will:

- keep records of safeguarding and online safety training
- review training needs regularly
- update training content in response to:
  - incidents or emerging trends
  - changes in statutory guidance
  - identified areas for development

This ensures training remains current, relevant and effective.

Monitoring arrangements

Bracken Hill School recognises that online safety is an evolving area of safeguarding and requires active monitoring, review and oversight to remain effective.

Monitoring arrangements are designed to ensure that online safety practice is robust, proportionate and responsive to risk.

Safeguarding oversight

The Designated Safeguarding Lead (DSL) is responsible for overseeing monitoring arrangements relating to online safety. This includes:

- reviewing safeguarding logs and incident records related to online safety

- reviewing alerts and concerns generated through monitoring systems
- identifying patterns, trends or emerging risks
- ensuring concerns are escalated appropriately

Where concerns indicate safeguarding risk, child protection procedures take precedence.

Filtering and monitoring review

Filtering and monitoring systems are reviewed:

- on a regular basis by senior leaders and technical staff
- in response to incidents or safeguarding concerns
- as part of the annual safeguarding review cycle

Review focuses on ensuring that systems:

- remain effective and proportionate
- do not create unintended safeguarding blind spots
- reflect the developmental and SEND needs of pupils

Assurance regarding filtering and monitoring is reported to the governing board.

Governance and accountability

The governing board provides strategic oversight by:

- receiving safeguarding reports that include online safety
- reviewing assurance provided by senior leaders and the DSL
- challenging and supporting leaders where appropriate

The governing board does not manage operational systems but ensures that effective arrangements are in place and reviewed.

Policy review

This Online Safety Policy will be:

- reviewed annually
- reviewed in response to significant incidents
- updated following changes in statutory guidance or identified risk

The policy review process incorporates:

- safeguarding incident analysis
- staff training feedback
- developments in technology and online risk

This ensures that online safety practice remains current and effective.

Links with other policies

This Online Safety Policy should be read in conjunction with the school's wider safeguarding, behaviour and information governance framework.

It is explicitly linked to the following policies:

- Child Protection and Safeguarding Policy
- Positive Behaviour Policy
- Staff Code of Conduct

- Acceptable Use Agreements (staff, pupils, volunteers and visitors)
- Data Protection Policy and Privacy Notices
- Searching, Screening and Confiscation Procedures
- Complaints Procedure
- Whistleblowing Policy

These policies work together to ensure a coherent, proportionate and effective approach to safeguarding, online safety, professional conduct and data protection.

Where concerns relate to safeguarding, the Child Protection and Safeguarding Policy takes precedence.