BECKFOOT TRUST

ONLINE SAFETY & IT USE POLICY

V10

September 2026

CREATING REMARKABLE SCHOOLS

Table of Contents

1.0 Policy statement 3
2.0 Scope and purpose 3
3.0 Overarching principles 4
4.0 Responsibilities and arrangements 6
5.0 Preventative action 12
6.0 Educating students about online safety 13
7.0 How to report a range of concerns 13
8.0 Educating parents/carers about online safety 14
9.0 Online safety trends 14
10.0 Cyber-bullying 15
11.0 Students using mobile devices in school 16
12.0 Acceptable use of the internet and devices 17
13.0 Staff using work devices outside school 20
14.0 Insurance requirements for work IT equipment and mobile devices 20
15.0 Filtering and monitoring 21
16.0 Generative artificial intelligence 22
17.0 Breaches of the policy 24
18.0 How our trust will respond to issues of misuse 24
19.0 Training 25
20.0 Policy monitoring arrangements 26
21.0 Review 26

1.0 Policy statement

1.1 Beckfoot Trust recognises that technology is an essential resource for teaching, learning, communication and the effective operation of our trust. It is also an inevitable feature in the everyday lives of children, young people and adults. Our trust is committed to ensuring that technology is used safely, securely, responsibly and appropriately across all schools and services.

1.2 Our trust recognises that the use of technology is a significant component of many safeguarding issues, including online abuse, child sexual exploitation, radicalisation, child-on-child abuse, sexual harassment, harmful content, AI-generated harm, phishing, financial scams and other forms of cyber-enabled harm. Technology can be used to facilitate abuse, exploitation, fraud, data loss, impersonation and other risks to pupils, staff and the wider trust community.

1.3 Beckfoot Trust aims to protect and educate pupils, staff and adults in their use of technology and has mechanisms in place to prevent, identify, report, intervene in and escalate concerns or incidents where appropriate. This includes safeguarding concerns, online safety incidents, cyber security incidents, suspected phishing, data breaches, misuse of systems and potential fraud.

1.4 Beckfoot Trust will maintain appropriate filtering, monitoring, access control, account security, malware protection, software update, secure configuration and incident response arrangements in line with relevant DfE standards, Keeping Children Safe in Education 2026, Cyber Essentials principles and Trust policies. Our trust will do all it reasonably can to limit pupils' exposure to harmful and inappropriate online material and to protect Trust systems, data and financial processes from misuse, compromise or fraud.

1.5 Our trust recognises that cyber-enabled fraud, including phishing, impersonation, social engineering, payment diversion, invoice fraud, credential theft and unauthorised access to finance or administrative systems, presents a risk to pupils, staff, families and the wider trust. Staff must report suspected fraud attempts, suspicious emails, compromised accounts, unusual payment requests or misuse of trust systems through the trust's agreed reporting procedures without delay. Trust systems, devices, email accounts and digital platforms must not be used for personal financial transactions or private financial gain. Any suspected fraud, attempted fraud or cyber-enabled financial abuse must be managed in accordance with this policy and our trust's anti-fraud policy.

2.0 Scope and purpose

2.1 This policy is based on the Department for Education's (DfE) latest statutory safeguarding guidance, Keeping Children Safe in Education. Also, the following DfE advice for schools:

- Meeting digital and technology standards in schools and colleges - GOV.UK (www.gov.uk)
- Mobile phones in schools - GOV.UK (www.gov.uk)
- Preventing and tackling bullying advice for headteachers, staff and governing bodies
- Cyberbullying: Advice for headteachers and school staff
- Relationships and sex education (RSE) and health education
- Searching, screening and confiscation in schools - GOV.UK (www.gov.uk)
- Harmful online challenges and online hoaxes - GOV.UK (www.gov.uk)
- Sharing nudes and semi-nudes: advice for education settings working with children and young people - GOV.UK (www.gov.uk)
- Prevent duty guidance: England and Wales (2023) - GOV.UK (www.gov.uk)

- Early years foundation stage (EYFS) statutory framework - GOV.UK (www.gov.uk)
- UKCIS_Early_Years_Online_Safety_Guidance_for_Practitioners 1_.pdf (publishing.service.gov.uk)
- Generative artificial intelligence (AI) in education - GOV.UK
- Keeping Children Safe in Education 2026 (effective from 1 September 2026)

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on students' electronic devices where they believe there is a 'good reason' to do so.

The policy also considers the National Curriculum: Computing programmes of study and the Online Safety Act 2023. KCSIE 2026 introduced several new areas which are expressly reflected in the policy. This policy should be read alongside Keeping Children Safe in Education 2026 and reflects the safeguarding expectations set out therein.

2.2 Links with other trust policies:

- child protection and safeguarding policy
- behaviour policy
- disciplinary policy
- data protection policy
- freedom of information policy and publication scheme
- privacy notices
- complaints policy
- code of conduct for employees

3.0 Overarching principles

3.1 Digital technology covers a wide range of systems, services, platforms, devices and online environments used both inside and outside school. It is important to recognise the constant and fast-paced evolution of technology and the safeguarding, cyber security, data protection and fraud risks that may arise from its use. These may include, but are not limited to:

- websites and internet search
- email, messaging, chat rooms and collaboration tools
- social media platforms, including Facebook, X, Snapchat, Instagram, TikTok, WhatsApp and Discord
- mobile phones, cameras and devices with imaging, recording, sharing, text, video or web functionality
- wearable technology, including smart watches and other connected devices
- making and receiving calls, messages or media through mobile or wearable devices
- online gaming, gaming platforms, live chat, streaming and in-game communication
- learning platforms, virtual learning environments and classroom apps
- cloud platforms, productivity tools, shared drives and online storage
- school management and administrative systems, including MIS, HR, finance, catering/payment and safeguarding systems
- user accounts, passwords, authentication and access rights
- personal devices, removable media and home networks where these interact with trust systems or school activity

- internet-connected equipment, including printers, CCTV, classroom screens, access control systems and other connected devices
- blogs, wikis, podcasting, video broadcasting, livestreaming, downloads and file sharing
- generative AI tools, chatbots, image/video/audio generation tools and other emerging technologies

3.2 The increasing accessibility of generative artificial intelligence tools presents emerging safeguarding, educational and cyber safety risks. Pupils may be able to access tools that generate text, images, audio, video or other content both in school and outside school. While these tools may support learning when used safely and appropriately, they can also produce inaccurate, misleading, biased, inappropriate or harmful material.

Our trust recognises that generative AI may create risks relating to misinformation, plagiarism, academic integrity, harmful content, impersonation, bullying, harassment, deepfakes, AI-generated intimate imagery, data privacy and online exploitation. Age restrictions, moderation systems and safety controls may not prevent pupils from accessing unsuitable content or using AI tools in harmful ways.

Staff should remain alert to the use or misuse of generative AI and should treat any concern involving AI-generated harmful content, manipulated media, impersonation, exploitation or inappropriate imagery as a safeguarding concern, reporting it in line with this policy and trust safeguarding procedures.

Beckfoot Trust recognises that children and young people now access digital technology as a normal part of everyday life, both in and outside school. Our trust is committed to educating, supporting and protecting pupils from these risks as part of its safeguarding responsibilities.

3.3 Online safety risks can be categorised into four areas of risk:

3.3.1 Content

Being exposed to illegal, inappropriate or harmful content, for example: pornography, fake news, racism, misogyny, online sexism, violence against women and girls (VAWG), harmful gender-based narratives, self-harm, suicide, anti-Semitism, radicalisation, extremism, misinformation, disinformation (including fake news), conspiracy theories and content promoted by harmful influencers that encourages harmful attitudes, abusive behaviours or discrimination. Concerns relating to online content that promotes misogyny, violence, coercive behaviours or gender-based harm should be treated as safeguarding concerns and responded to in line with the school's child protection and safeguarding procedures

3.3.2 Contact

Being subjected to harmful online interaction with other users or generative AI applications that simulate this; 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

3.3.3 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 self-generated intimate images and/or videos including those generated using AI e.g. deepfakes, sharing other explicit images and online bullying, and

3.3.4 Commerce

Risks such as online gambling, inappropriate advertising, phishing and or financial scams. If you feel your pupils, students or staff are at risk, please report it to the Anti-Phishing Working Group (https://apwg.org/).

Types of online harm may include cyberbullying, misogyny, trolling, or online harrassment, making or sharing of nudes or semi-nudes, online grooming or radicalisation, access to harmful content, including self-harm or extremist material or exploitation through gaming or social media platforms.

3.4 Artificial intelligence

Our trust recognises the increasing use of artificial intelligence (AI) technologies across education and wider society. While AI offers opportunities to enhance teaching, learning and administration, it also presents emerging safeguarding risks. Our trust is committed to ensuring that:

- the use of AI does not compromise the safety and wellbeing of pupils
- safeguarding principles apply equally to AI-enabled and digital environments
- staff always exercise professional judgement in using AI or encouraging its usage
- staff will remain alert to how students may use AI, especially in ways that could impact online safety, data privacy, or wellbeing. This includes emerging risks such as AI-generated bullying - for example, the creation of fake images (deepfakes), harmful content using chatbots, or AI-edited videos designed to harass, humiliate, or target individuals.

In line with KCSIE, online safety is a whole-school responsibility embedded within safeguarding culture, leadership oversight and the curriculum. The Trust is committed to ensuring that all children are protected from harmful online content, contact, conduct and commerce while being equipped with the knowledge and skills to use technology safely and responsibly.

4.0 Responsibilities and arrangements

4.1 The trust board and CEO

The trust board has overall responsibility for monitoring this policy and holding the CEO to account for its implementation, responsibility for oversight of **digital safeguarding, cyber security, fraud risk and DfE standards compliance** (including the scrutiny of filtering and monitoring data).

Online safety will be audited as part of the external safeguarding review, and these reports will be shared with the trust board.

All board members will:

- ensure that they have read and understand this policy.
- agree and adhere to the terms on acceptable use of trust IT systems and the internet (Appendix 2).

There is a named trustee who has responsibility for safeguarding and child protection. This responsibility includes cyber and online safety.

4.2 The safeguarding and cyber security trustee

The role of the safeguarding and cyber security trustee is to seek assurance on behalf of the trust board that safeguarding, online safety, digital technology, cyber security and cyber-enabled fraud risks are identified, understood and managed effectively across the Trust. The role provides strategic oversight and challenge but does not replace the operational responsibilities of the CEO, executive leaders, DSLs, IT leaders or school leaders. The role includes:

- understanding the requirements of the Governance Handbook, Keeping Children Safe in Education, relevant DfE digital and technology standards, Cyber Essentials principles and trust safeguarding, IT, data protection and anti-fraud policies
- seeking assurance, supporting and challenging the executive member for safeguarding, the trust safeguarding lead, DSLs and IT leaders on the effectiveness of safeguarding, online safety, filtering and monitoring, cyber security and fraud prevention arrangements
- confirming that consistent and compliant safeguarding and online safety practice takes place across our trust, including appropriate arrangements for vulnerable children, victims of abuse and pupils with SEND
- seeking assurance that digital systems, infrastructure, user accounts, data, devices and cloud services are secure, resilient and appropriately governed
- seeking assurance that our trust is working towards relevant DfE digital and technology standards, including digital leadership and governance, filtering and monitoring, cyber security, broadband, wireless networks and network switching
- seeking assurance that cyber essentials-style controls are in place and reviewed, including access control, secure configuration, malware protection, software updates and boundary protection
- seeking assurance that cyber-enabled fraud risks, including phishing, impersonation, social engineering, payment diversion, invoice fraud, compromised accounts and financial system misuse, are understood, reported and escalated in line with Trust procedures and the anti-fraud policy
- ensuring that incidents involving technology are considered for their safeguarding, cyber security, data protection, operational, financial and reputational impact.
- reporting to the board of trustees on safeguarding, online safety, cyber security, filtering and monitoring, fraud-related risks, assurance activity, significant incidents, trends and areas for improvement

The safeguarding and cyber security trustee will meet regularly with the executive member for safeguarding, the trust safeguarding lead and relevant IT leaders to review safeguarding, online safety, filtering and monitoring, cyber security and cyber-enabled fraud risks, and to agree steps to continuously improve practice across our trust.

4.3 Executive responsibility for safeguarding

The executive leader for safeguarding is accountable for ensuring that our trust meets its statutory safeguarding obligations under **Keeping Children Safe in Education (KCSIE) 2026**, **Working Together to Safeguard Children**, and other relevant safeguarding legislation and guidance, including safeguarding risks arising from digital technology, cyber security incidents and cyber-enabled fraud. They will:

- ensure schools maintain safeguarding procedures that incorporate online safety, filtering and monitoring, cyber-enabled harm, cyber security incidents and technology-related safeguarding risks
- ensure DSLs understand and fulfil their responsibilities for online safety, including the review and investigation of filtering and monitoring concerns, alerts and safeguarding incidents
- ensure suitable procedures are in place for staff, pupils, parents, carers and visitors to report safeguarding concerns, including concerns relating to online activity, harmful content, grooming, exploitation, cyberbullying, AI-generated content, fraud and cyber-enabled abuse
- ensure safeguarding risk assessments consider the use of digital technologies, social media, messaging platforms, gaming services, artificial intelligence, cloud services and emerging technologies

- work with the executive leader responsible for IT to ensure filtering and monitoring arrangements are appropriate, effective and proportionate to identified risks.
- Ensure safeguarding reviews consider:
    - pupil vulnerability and risk profiles, including SEND and EAL pupils
    - local contextual safeguarding risks
    - safeguarding incident trends
    - filtering and monitoring reports
    - cyber-related safeguarding incidents
    - emerging online and technology-enabled risks
- ensure safeguarding records, filtering and monitoring reports, cyber incidents and lessons learned are reviewed and used to inform training, curriculum planning, policy development and continuous improvement
- ensure safeguarding training includes online safety, cyber-enabled harm, artificial intelligence risks, phishing, fraud awareness and emerging technology risks
- provide assurance to the CEO and trust board that schools have appropriate safeguarding procedures and controls in place and that statutory safeguarding duties are being met

4.4 Executive responsibility for information technology, cyber security and digital services

The executive leader for IT is accountable for ensuring that trust technology services, cyber security controls and digital systems support the trust's safeguarding responsibilities and comply with **KCSIE 2026**, **DfE Digital and Technology Standards**, **Cyber Essentials**, **Cyber Essentials Plus** (where adopted), data protection requirements and other applicable cyber security guidance. They will:

- provide strategic leadership for information technology, cyber security, digital resilience and fraud prevention across our trust
- ensure technology systems, infrastructure and services support the safeguarding objectives of our trust.
- ensure cyber security controls are implemented and maintained in line with DfE digital and technology standards, cyber essentials requirements and recognised good practice
- ensure effective filtering and monitoring systems are implemented, maintained and reviewed across our trust to support safeguarding requirements
- work jointly with the executive leader for safeguarding to review the effectiveness of filtering and monitoring arrangements and ensure identified risks are addressed.
- ensure headteachers and DSLs have access to appropriate filtering and monitoring reports, guidance and support to enable safeguarding concerns to be investigated and managed effectively
- ensure clear procedures exist for responding to:
    - filtering and monitoring alerts
    - cyber security incidents
    - attempted or successful cyber-attacks
    - compromise of user accounts
    - misuse of Trust systems
    - data breaches
    - cyber-enabled fraud affecting pupils, staff or trust operations
- ensure cyber security risks that may impact pupil safety or safeguarding are identified, assessed, escalated and communicated to safeguarding leaders
- ensure appropriate technical controls are in place

- ensure regular review of filtering and monitoring provision, taking account of:
    - pupil risk profiles and vulnerabilities
    - safeguarding risks and incidents
    - curriculum requirements
    - digital resilience of pupils
    - emerging technologies
    - AI-enabled risks
    - the effectiveness of current controls
- ensure cyber security awareness and fraud prevention training is available for staff and aligned with safeguarding responsibilities
- ensure suitable arrangements are in place for IT teams, DSLs, headteachers, data protection leads and external suppliers to work together when safeguarding concerns involve digital systems or technology
- ensure cyber security incidents, filtering and monitoring outcomes, system misuse and fraud incidents are recorded, investigated and reported through appropriate governance channels
- provide assurance to the CEO and trust board that trust systems appropriately support safeguarding obligations, and that cyber security and fraud prevention controls remain effective.

4.5 Service delivery manager: safeguarding, cyber security and fraud prevention

The service delivery manager is responsible for the operational implementation, monitoring and continual improvement of our trust's technical controls for safeguarding, cyber security and fraud prevention. The role ensures that IT services operate in accordance with trust policies, the DfE digital and technology standards, KCSIE 2026, cyber essentials requirements and relevant data protection obligations. They will

- implement and maintain secure, resilient and compliant trust technology services, including identity management, endpoint security, network security, vulnerability management, patching, monitoring, backup and recovery, in line with DfE standards and cyber essentials
- ensure trust systems, storage and digital services meet the requirements of DfE Cyber Security, Filtering and Monitoring, and Servers and Storage Standards
- manage and review filtering, monitoring and technical safeguarding controls, working with LGfL and Smoothwall to protect users from harmful content, monitor emerging risks and maintain appropriate block and allow lists
- conduct regular security, safeguarding and compliance reviews, including an annual online safety, filtering and monitoring, and cyber security assessment, ensuring risks and improvement actions are documented and addressed.
- implement and maintain effective fraud prevention controls, including the detection, investigation, escalation and reporting of phishing, impersonation, account compromise, financial scams and other cyber-enabled fraud risks.
- provide technical leadership, reporting and assurance to headteachers, DSLs and trust leaders, ensuring compliance with KCSIE 2026, DfE Digital and Technology Standards, Cyber Essentials, and trust safeguarding, cyber security and fraud prevention policies.
- work with the trust safeguarding lead to review the web filter policy and confirm that each policy rule appropriately defines:
    - **who:** the individual user or user group to whom the policy applies
    - **what:** the web content category or group of categories covered by the policy
    - **where:** the network location, IP address or IP range to which the policy applies
    - **when:** the times during which the policy is active

- **action:** how Smoothwall will allow, block, monitor, warn or otherwise respond to the activity

- ensure changes to filtering policies are authorised, documented, tested and communicated to relevant safeguarding and school leaders.

4.6 Headteacher

The headteacher will:

- ensure safeguarding and online safety policies are consistently implemented across the school, embedded within the curriculum, culture and daily operations, and supported by effective procedures for identifying, recording, reporting and escalating safeguarding concerns, including technology-enabled harm
- support the designated safeguarding lead (DSL) in discharging their safeguarding and online safety responsibilities and ensure sufficient time, resources and leadership support are available
- ensure safeguarding education, including online safety, is adapted where necessary to meet the needs of vulnerable pupils, victims of abuse, and pupils with special educational needs and disabilities (SEND), recognising that a personalised and contextualised approach may be required
- ensure concerns identified through filtering and monitoring systems are reviewed and acted upon through the school's safeguarding procedures
- monitor the effectiveness of safeguarding and online safety arrangements and take action to address identified risks, gaps or areas for improvement

4.7 Designated safeguarding lead (DSL)

The designated safeguarding lead (DSL) is responsible for leading safeguarding and online safety within the school in accordance with KCSIE 2026, the DfE Filtering and Monitoring Standards for Schools and Colleges, and trust safeguarding policies. They will:

- take lead responsibility for safeguarding, child protection and online safety, ensuring safeguarding arrangements are effective, compliant and embedded across the school
- oversee and act upon safeguarding concerns, filtering and monitoring reports, online safety incidents and technology-enabled safeguarding risks, ensuring appropriate recording, investigation, escalation and resolution
- work closely with the headteacher, IT teams, service delivery manager and external providers to ensure filtering and monitoring systems are effective and that safeguarding concerns identified through technical systems are appropriately managed
- ensure online safety incidents, cyberbullying, harmful online behaviour, AI-related safeguarding concerns and other technology-enabled risks are managed in accordance with safeguarding and child protection procedures
- review safeguarding, filtering and monitoring information to identify trends, risks and emerging concerns, and use this information to inform safeguarding actions, risk assessments and pupil support
- ensure staff receive appropriate safeguarding and online safety guidance and training, including emerging risks associated with digital technology, cyber-enabled harm and artificial intelligence
- work with external agencies, safeguarding partners and specialist providers where safeguarding concerns require multi-agency support or intervention
- provide regular reports and assurance to the headteacher and LSC on safeguarding, online safety, filtering and monitoring effectiveness, significant incidents, emerging risks and improvement actions

4.8 All staff, volunteers, contractors, visitors and agency staff (this list is not intended to be exhaustive)

All staff, volunteers, contractors and agency staff have a responsibility to safeguard children, promote online safety, prevent cyber-enabled harm, and comply with this policy, KCSIE 2026 and trust procedures. They will:

- understand, comply with and consistently implement this policy, the trust's acceptable use requirements, safeguarding procedures and online safety expectations
- maintain an awareness of safeguarding, online safety, cyber security and emerging technology risks, including risks associated with artificial intelligence (AI), and contribute to creating a culture where safeguarding is everyone's responsibility
- immediately report safeguarding, online safety, cyber security or technical concerns, including where they:
    - witness or suspect access to inappropriate or harmful material
    - are able to access inappropriate material
    - identify unusual activity resulting from legitimate teaching and learning activities
    - become aware of failures, weaknesses or misuse of filtering, monitoring or other IT systems
    - identify restrictions that unreasonably impact educational or business activities
    - discover methods used to bypass filtering or monitoring controls
- work with the designated safeguarding lead (DSL) to ensure safeguarding, online safety and technology-related incidents are appropriately recorded, investigated, managed and escalated
- respond appropriately to all safeguarding concerns, including online abuse, cyberbullying, child-on-child abuse, sexual violence and sexual harassment, maintaining an attitude of "it is happening here"
- understand the additional online risks that may affect vulnerable children and pupils with special educational needs and disabilities (SEND), and support them to remain safe online
- use trust technology, communication systems and digital resources responsibly and in accordance with trust policies and acceptable use requirements
- use only trust-approved devices and systems for capturing, storing or processing images, video or other information relating to pupils, and ensure such information is stored securely on trust-managed systems
- not use personal communication devices in areas where pupils are present unless expressly authorised by the headteacher in exceptional circumstances
- remain alert to the potential misuse of AI technologies, including deepfakes, synthetic audio, AI-generated imagery, impersonation, manipulated evidence and other harmful or exploitative content
- immediately report any concerns involving AI-generated content, online exploitation, cyber-enabled harm or technology-related safeguarding risks to the designated safeguarding lead.

4.9 Families

Beckfoot Trust asks that all of our families to support the aims of this policy by:

- ensuring their child (where age appropriate) has read, understood and agreed to the terms on acceptable use of IT and internet
- helping and supporting the school in promoting online safety with their children
- discussing online safety concerns with their children, showing an interest in how they are using technology, and encouraging them to behave safely and responsibly when using technology
- consulting with the school if they have any concerns about their child’s use of technology

- supporting Beckfoot Trust's approach to online safety and not deliberately post comments or upload any images, sounds or text that could upset or offend any member of the school community or bring the school into disrepute

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

- UK Safer Internet Centre - What are the Issues?
- Childnet International - Hot Topics
- Childnet International - Parent Factsheet
- Safer Internet Day 2025 Film for Parents and Carers
- Online Safety Basics - National Cybersecurity Alliance
- Parent Zone - Working Towards a Safer Digital World TALK Checklist by the Internet Watch Foundation
- TALK Checklist by Internet Watch Foundation | Home

4.10 Pupils

All pupils at in our schools are expected to:

- take responsibility for their own and each other's' safe and responsible use of technology wherever it is being used, including judging the risks posed by the personal technology owned and used by them outside of school
- ensure they respect the feelings, rights and values of other pupils in their use of technology at school and at home
- understand what action should be taken if they feel worried, uncomfortable, vulnerable or at risk whilst using technology, or if they know of someone to whom this is happening
- report all online safety incidents to appropriate members of staff in school
- discuss online safety issues with family and friends in an open and honest way
- know, understand and follow school policies on the use of technology to an age-appropriate level
- support their school approach to online safety and not deliberately post comments or upload any images, sounds or text that could upset or offend any member of the school community or bring the school into disrepute.

See the pupil acceptable use policy for more details.

4.11 Visitors and members of the community

Visitors and members of the community agree to the terms and conditions of the acceptable use policy (see Appendix 2) when signing in at reception. Safeguarding information sheets are distributed on arrival to make visitors aware of the trust's IT systems. Internet access to guest WIFI is time limited and accessible through a code distributed on arrival.

5.0 Preventative action

5.1 There are four stages of prevention and action when managing online safeguarding.

- **Education** – school's preventative curriculums help pupils understand how to stay safe online and why certain content is unacceptable.
- **Prevention** – all staff are vigilant and don't rely on technical monitoring.
- **Reaction** – all staff should address unacceptable and unsafe behaviour, and the DSL should investigate any online safeguarding incidents.

- **Reporting and monitoring** – leaders should review reports so that strategies are put in place to ensure safe use of technology in our schools.

5.2 The DfE filtering and monitoring standards for schools and colleges states clearly that technical monitoring systems do not stop unsafe activities on a device or online. Staff should:

- provide effective supervision
- take steps to maintain awareness of how devices are being used by pupils
- report any safeguarding concerns to the DSL

6.0 Educating students about online safety

Students will be taught about online safety as part of the curriculum.

6.1 In key stage 1, students will be taught to:

- use technology safely and respectfully, keeping personal information private
- identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

6.2 In key stage 2, students will be taught to:

- use technology safely, respectfully, and responsibly
- recognise acceptable and unacceptable behaviour
- identify a range of ways to report concerns about content and contact

6.3 In key stage 3, students will be taught to:

- understand a range of ways to use technology safely, respectfully, responsibly, and securely, including protecting their online identity and privacy
- recognise inappropriate content, contact, and conduct, and know how to report concerns

6.4 In key stage 4, students will be taught:

- to understand how changes in technology affect safety, including new ways to protect their online privacy and identity
- how to report a range of concerns

6.5 Individual school curriculums should address online safety through the four categories of risk; content, contact, conduct and commerce (See Section 3).

The safe use of social media and the internet will also be covered in other subjects where relevant.

The school will use assemblies to raise students' awareness of the dangers that can be encountered online and may also invite speakers to talk to students about this.

Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.

7.0 How to report a range of concerns

7.1 Beckfoot Trust encourages all members of the school community to report concerns relating to online safety, inappropriate content, online abuse, cyberbullying, harmful online interactions, exploitation, or any other behaviour that may place a child or young person at risk.

7.2 Pupils should be encouraged to seek help and report concerns as soon as possible. This may be through:

- speaking to a trusted adult in school
- speaking to their tutor, class teacher, pastoral leader or head of year
- reporting directly to the designated safeguarding lead (DSL) or a deputy DSL
- using any school reporting systems made available to pupils

7.3 Where concerns relate to online abuse, exploitation, inappropriate contact, sexual abuse, or attempts by others to groom or manipulate a child online, the matter should be referred immediately to the DSL who will determine appropriate safeguarding action in line with the trust child protection and safeguarding policy.

7.4 Pupils, parents/carers and staff may also access external reporting and support services where appropriate, including:

- CEOP (Child Exploitation and Online Protection Command) for reporting online grooming, exploitation or abuse
- **Report Remove**, which supports children and young people to report and seek the removal of nude or semi-nude images shared online
- **Childline**, which provides confidential advice and support for children and young people
- the relevant social media, gaming or online platform reporting tools
- the police, where there is an immediate risk of harm or where criminal offences may have been committed

7.5 Staff must report all online safety concerns, safeguarding concerns and filtering and monitoring concerns in accordance with local safeguarding procedures and the trust child protection and safeguarding policy. Concerns should be recorded promptly using the school's agreed recording system.

7.6 Our trust recognises that online concerns may occur both within and outside school. Any concern that may impact a pupil's welfare, safety or education will be taken seriously and responded to in accordance with safeguarding procedures, regardless of where or when the incident occurred.

8.0 Educating parents/carers about online safety

8.1 Schools will raise parents' awareness of internet safety in various ways e.g. parents' evenings, letters, news items etc. through the school website or parental communication systems.

8.2 If parents/carers have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher and/or the DSL. Concerns or queries about this policy can be raised with any member of staff or the headteacher.

8.3 Schools may need to seek further advice if they are concerned parents/carers are not addressing online safety.

9.0 Online safety trends

9.1 At Beckfoot Trust, we are mindful that the online world is ever developing, and we recognise that we must be vigilant in being aware of and responding to new risks that may harm our pupils. For example, the increasing prevalence of self-generative artificial intelligence is a growing concern, with pupils potentially having access to tools that generate text and images at home or in school. These tools not only represent a challenge in terms of accuracy when young people are genuinely looking for

information, but also in terms of plagiarism for teachers, and above all, safety. None of the mainstream tools have end-user safety settings and will easily produce inappropriate material despite the age limits that are in place on them.

Against this background, the Ofcom 'Children and parents: media use and attitudes report 2024' has shown that an increasing number of younger children are having a presence online, there has been a rise in online gaming activity across children of all ages, and children have been twice as likely as adults to have used artificial intelligence technology.

Beckfoot Trust recognises the increasing influence of online personalities, influencers and communities that may promote harmful attitudes, including misogyny, online sexism, violence against women and girls, coercive control, discrimination and gender-based abuse. Our trust will ensure that pupils are supported to critically evaluate online content, recognise harmful narratives and understand how to report concerns where online content may place themselves or others at risk.

9.2 We are aware many children, and young adults struggle to identify harmful content and challenges online. Incidents which affect the wellbeing and safeguarding of our students include:

- sharing inappropriate images via chat groups out of school
- incidents of online bullying using chat groups and messaging apps
- pupils playing games that are not age appropriate
- pupils contacting / being contacted by unknown individuals using online game platforms
- searching for inappropriate terms using school resources, including online gaming platforms
- YouTube videos
- pupils following online trends and dares using platforms such as TikTok

9.3 We are mindful other issues that may affect our schools include:

- an increase in the number fights being filmed and shared
- an increase in the cases of self-harm and sexual abuse being coerced with threats of violence
- an increase in unpleasant and even cyberbullying behaviour between pupils through social media apps
- an increase in the number of fake profiles causing issues including:
    - where the school logo and/or name have been used to share inappropriate content about students
    - spreading of defamatory allegations about staff
    - using fake profiles to bully others (sometimes even pretending to be one student to bully another student)

Risk is constantly reviewed at both school and centrally to try to mitigate against concerns as much as possible.

10.0 Cyber-bullying

Definition: Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.)

10.1 Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that students understand what it is and what to do if they become aware of it happening to them or others. We will ensure that students know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with students, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Class teachers and tutors will discuss cyber-bullying with their tutor/registration groups, and the issue will be addressed in assemblies.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, board members and volunteers (where appropriate) receive training on cyber-bullying, its impact, and ways to support students, as part of safeguarding training (see section 19 for more detail).

The school also sends information on cyber-bullying to parents/carers so that they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate, or harmful material has been spread among students, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will consider whether the incident should be reported to the police if it involves illegal material and will work with external services if it is deemed necessary to do so.

11.0 Students using mobile devices in school

It is recognised that extensive mobile device use is detrimental to children's mental health and wellbeing. However, we understand that many families want children to have a phone for safety reasons when travelling to and from school. Beckfoot Trust schools operate as phone-free environments except in approved circumstances determined by school leaders. Mobile device usage in lesson time or at social time is not permitted, with the exception of post-16 students or for students with a medical condition that is monitored via an app on a mobile device). Schools will maintain and publish local arrangements regarding pupil mobile phone use in accordance with DfE mobile phone guidance in local behaviour protocols.

11.1 Examining electronic devices

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on students' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- cause harm
- disrupt teaching
- break any of the school rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

- delete that material, or
- retain it as evidence (of a criminal offence or a breach of school discipline), and/or

- report it to the police*

*Staff may also confiscate devices for evidence to hand to the police, if a pupil discloses that they are being abused and that this abuse includes an online element.

Any searching of students will be carried out in line with:

- the DfE's latest guidance on screening, searching and confiscation
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

Any complaints about searching for or deleting inappropriate images or files on students' electronic devices will be dealt with through the school complaints procedure.

12.0 Acceptable use of the internet and devices

All students, parents, staff, volunteers, and board members are expected to sign an agreement regarding the acceptable use of the trust IT systems and the internet (Appendices 1 and 2). Visitors will be expected to read and agree to the trust terms on acceptable use if relevant.

Use of the trust internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor and filter the websites visited by students, staff, volunteers, board members and visitors (where relevant) to ensure they comply with the above.

More information is set out in the acceptable use agreements in Appendices 1 and 2.

12.1 Employees personal use of social media

Employees must not identify themselves as employees of the trust in their personal 'social' online spaces such a X and Facebook. This is to prevent information on these sites from being linked with our trust and to safeguard the privacy of staff members, particularly those involved in providing sensitive frontline services.

Where employees choose to present themselves in their professional role on sites such as Linked In, they must ensure that any posts do not have the potential to bring the trust, school or profession into disrepute. For safeguarding reasons, as a trust, we do not engage with X (formerly Twitter), and we do not encourage our students to interact with us on this forum. Our code of conduct policy reminds colleagues of their online responsibilities, particularly in relation to contact with children and families. All employees are also reminded in this policy that they must avoid all electronic communication that might be misconstrued in a way that could damage our trust's reputation, even indirectly. Employees have a duty to report any activity from our students or other colleagues that is of concern.

Our trust does not expect employees to discontinue contact with their family members via personal social media once the trust starts providing services for them. However, any information employees obtain in the course of their employment must not be used for personal gain or be passed on to others who may use it in such a way.

- Employees must not have any contact with pupils' family members through personal social media if that contact is likely to constitute a conflict of interest or call into question their objectivity.
- Employees must decline 'friend requests' from pupils they receive in their personal social media accounts. Instead, if they receive such requests from pupils of any school who are not family members, they may discuss these in general terms in class where the pupils attend the school and signpost pupils to become 'friends' of the official school site if there is one.

- Information employees have access to as part of their employment, including personal information about pupils and their family members, colleagues, and other parties and trust corporate information must not be discussed on their personal online space.
- Photographs, videos, or any other types of images of pupils and their families or images depicting employees wearing clothing with school logos on must not be published on personal web space.
- Trust/school email addresses and other official contact details must not be used for setting up personal social media accounts or to communicate through such media.
- The trust only permits limited personal use of social media during designated break points. However, employees are expected to devote their contracted hours of work to their professional duties, and, in practice, personal use of the internet should not be in the trust's time. This is subject to:
    - not depriving pupils of the use of the equipment and/or
    - not interfering with the proper performance of employee's duties
- Caution is advised when inviting work colleagues to be 'friends' in personal social networking sites. Employees are advised that they set the privacy levels of their personal sites as strictly as they can and to opt out of public listings on social networking sites to protect their own privacy.
- Employees should keep their passwords confidential, change them often and be careful about what is posted online. It is not appropriate to reveal home addresses, telephone numbers and other personal information.

12.2 Using social media on behalf of the trust

- Employees can only use official trust sites for communicating with pupils or to enable pupils to communicate with one another.
- Employees should seek permission from the headteacher before creating an official trust related site explaining their business reasons for doing so.
- Any official trust sites created must not breach the terms and conditions of social media service providers, particularly regarding minimum age requirements.
- Employees must always act in the best interests of children and young people when creating, participating in or contributing content to social media sites.
- If you are contacted for comments about the trust for publication anywhere, including in any **social media outlet please direct the enquiry to the headteacher**.

12.3 Use of trust IT

Staff who use the trust's IT and communication systems must:

- use it responsibly
- keep it safe
- keep passwords confidential and must report any breach of password confidentiality to the headteacher or nominated IT team as soon as possible.
- report any known breaches of this policy, including any inappropriate images or other material which may be discovered on the trust's IT systems.
- report to the headteacher or designated safeguarding officer any vulnerabilities affecting child protection in the trust's IT and communications systems.
- not install software on the trust's equipment unless authorised by the IT leadership.
- comply with any IT security procedures governing the use of systems in the school, including anti-virus measures.
- ensure that it is used in compliance with this policy.

Any equipment provided to a trust employee is provided for their sole use. Any use of the equipment by family or friends is not permitted and any misuse of the equipment by unauthorised users will be the responsibility of the staff member.

12.4 Email and communications systems usage

The following uses of IT are prohibited, may amount to gross misconduct, and could result in dismissal.

- to make, to gain access to, or for the publication and distribution of inappropriate sexual material, including text and/or images, or other material that may deprave or corrupt those likely to read or see it
- to make, to gain access to, and/or for the publication and distribution of material promoting homophobia or racial or religious hatred
- for the purpose of bullying or harassment, or for or in connection with discrimination on the grounds of gender, race, religion, disability, age or sexual orientation
- for the publication and/or distribution of libellous statements or material which defames or degrades others
- for the publication of material that brings the trust or its pupils or employees into disrepute
- for the publication and distribution of personal data without authorisation
- where the content of the email correspondence is unlawful
- to participate in on-line gambling
- where the use infringes copyright law
- To gain unauthorised access to internal or external computer systems (commonly known as hacking)
- to create or deliberately distribute IT or communications systems viruses
- to record or monitor telephone or email communications without the express approval of the trust. In no case will such recording, or monitoring be permitted unless it has been established that such action is in full compliance will the relevant legislation i.e. the Regulation of Investigatory Powers Act 2000.
- to participate in “chain” e-mail correspondence
- in pursuance of personal business or financial interests or political activities (excluding the legitimate activities of recognised trade unions).

Please see the disciplinary policy for further guidance.

12.5 Data protection and fraud prevention

All staff, volunteers, contractors and agency workers are responsible for protecting trust information and resources by complying with data protection requirements and remaining vigilant to fraud risks.

Staff will:

- handle personal, confidential and sensitive information in accordance with UK GDPR, the Data Protection Act 2018 and trust policies, ensuring information is only accessed, used, shared and stored for legitimate educational and business purposes
- protect personal data from unauthorised access, loss, disclosure, alteration or destruction, and immediately report any actual or suspected data breaches in accordance with trust procedures
- ensure confidential information is only shared with authorised individuals and through approved trust systems and communication channels

- Exercise caution when receiving emails, messages, telephone calls or requests involving personal information, financial transactions, account changes or sensitive data, recognising that these may be phishing, impersonation or fraud attempts.
- verify the authenticity of requests involving payments, supplier details, payroll information, banking changes or the release of sensitive information before taking action
- immediately report suspected fraud, phishing attempts, account compromise, financial scams, data protection concerns or other suspicious activity through the trust's reporting procedures.
- complete mandatory data protection and fraud awareness training and apply the principles of good information handling and fraud prevention in everyday practice
- support a culture of vigilance where protecting personal information, public funds and trust resources is everyone's responsibility

13.0 Staff using work devices outside school

13.1 Staff members using a work device outside school must not install any unauthorised software on the device and must not use the device in any way which would violate the trust's terms of acceptable use, as set out in Appendix 2.

Staff must ensure that their work device is secure and password-protected, preferably encrypted where possible and practical, and that they do not share their password with others. Any USB, disks or portable hard drives devices containing trust or school data must be encrypted/password protected.
Staff must take all reasonable steps to ensure the security of their work device when using it outside school. For example, but not limited to:

- not connecting to an unprotected WIFI connection
- using the device where the screen may be visible by others when accessing personal data e.g. student and staff records:
- making sure the device is locked if left unattended
- not sharing the device among family or friends

14.0 Insurance requirements for work IT equipment and mobile devices

14.1 It is a condition of our trust insurance policy that whenever hardware e.g., laptops and mobile devices are left in an unattended vehicle, they must be kept out of sight in a luggage compartment, glove compartment, or similar container and all windows or openings must be closed and all doors locked. If the items are left in an unattended vehicle overnight, the vehicle must be in a secure or attended garage or compound. In the event of a theft, failure to adhere to these conditions will result in an insurance claim being refused.

If staff have any concerns over the security of their device, they must seek advice from the IT team.

Work devices must be used solely for work activities.

Loss or theft of any work equipment must be reported to the police immediately and IT Team or cluster business manager immediately. Full details of the loss or theft will be required together with the crime reference number for insurance purposes.

15.0 Filtering and monitoring

15.1 Beckfoot Trust recognises that filtering and monitoring systems are an important component of safeguarding and play a key role in protecting children from online harm. Our trust will do all that it reasonably can to limit children's exposure to illegal, inappropriate and potentially harmful online content when using trust devices, systems and networks. Filtering and monitoring arrangements form part of our trust's wider safeguarding framework and support the prevention, identification and management of online safety risks. [gov.uk], [gov.uk]

15.2 Roles and responsibilities

The trust board is responsible for ensuring that appropriate filtering and monitoring systems are in place and that their effectiveness is reviewed regularly. The board will seek assurance that safeguarding, leadership and technical staff are working together to maintain effective arrangements. [gov.uk], [gov.uk]

The designated senior leader responsible for filtering and monitoring will oversee the effectiveness of filtering and monitoring arrangements and ensure appropriate governance, reporting and review processes are in place. [saferinternet.org.uk], [gov.uk]

The designated safeguarding lead (DSL) will work closely with IT staff and service providers to:

- understand how filtering and monitoring systems operate
- review safeguarding alerts and reports
- ensure appropriate safeguarding responses are implemented
- escalate concerns where necessary
- consider emerging risks and trends affecting pupils [gov.uk], [saferinternet.org.uk]

Technical staff and service providers will ensure that filtering and monitoring systems are configured, maintained and reviewed in accordance with statutory guidance and our trust's safeguarding requirements. [gov.uk]

15.3 Filtering

Filtering systems will:

- block access to illegal content, including child sexual abuse material
- reduce access to inappropriate, harmful or unsuitable content
- support age-appropriate access to online resources
- be applied consistently across trust-managed devices, operating systems and internet connections where reasonably possible
- be reviewed regularly to ensure they remain effective and proportionate [gov.uk], [gov.uk]

The trust recognises that filtering is not an alternative to effective supervision, education and safeguarding practices and that no filtering system can completely eliminate online risk. [gov.uk]

15.4 Monitoring

Monitoring systems provide an additional layer of safeguarding by identifying indicators of potential risk or harm. Monitoring arrangements may include the review of online activity, searches, communications, device usage and other indicators of safeguarding concern where appropriate and lawful. [gov.uk]

Monitoring systems may identify concerns relating to:

- child-on-child abuse.
- bullying and cyberbullying.
- self-harm or suicidal ideation.
- radicalisation and extremism.
- sexual harassment or abuse.
- safeguarding disclosures.
- attempts to access harmful content.
- AI-generated harmful or inappropriate content. [gov.uk], [gov.uk]

Safeguarding alerts generated through monitoring systems will be reviewed promptly and responded to in accordance with our trust's child protection and safeguarding policy.

15.5 Emerging technologies and artificial intelligence

Our trust recognises that online risks continue to evolve and that filtering and monitoring systems must be capable of responding to emerging technologies, including generative artificial intelligence.

Where reasonably practicable, filtering and monitoring arrangements will be reviewed to identify risks associated with:

- AI-generated harmful content
- deepfake images, videos and audio
- nudification tools and AI-generated intimate imagery
- AI-enabled bullying or harassment
- misinformation, disinformation and manipulated content
- online exploitation facilitated through AI technologies. [safeguard-hub.org], [saferinternet.org.uk], [gov.uk]

15.6 Annual review of effectiveness

Our trust will undertake and document a formal review of the effectiveness of its filtering and monitoring arrangements at least once every academic year.

This review will be led by the central leader responsible for filtering and monitoring, supported by the designated safeguarding leads and IT support. The review will consider:

- the effectiveness of current filtering and monitoring systems
- safeguarding incidents and trends
- emerging online risks
- the age, needs and vulnerability of pupils, including pupils with SEND
- new technologies and AI-related risks
- recommendations arising from safeguarding audits, inspections or reviews [safeblog.lgfl.net], [saferinternet.org.uk], [gov.uk]
- reviews of filtering and monitoring will consider risks associated with AI-generated and personalised content and whether current solutions remain effective

The effectiveness of filtering and monitoring arrangements will be formally reviewed and documented at least annually, with outcomes reported to trustees.

16.0 Generative artificial intelligence

Any use of generative AI by staff and students should be carefully considered and assessed, evaluating the benefits and risks of use in the education setting. The intended use should be specified and have clear

benefits that outweigh the risks. Safety should not be compromised. Schools should also consider that there may be uses of generative AI by staff or students that have not been explicitly approved or adopted and monitor the suitability and safety of this.

Our trust follows the age restriction guidance of AI platforms, and we do not make these solutions available to students in our schools.

Staff have access to some generative AI tools through third party applications we use or by unfiltering Chat GPT. We expect staff to consider the following:

- personal data must be always protected and must never be shared with platforms outside of our organisation (eg. uploading a spreadsheet to ChatGPT for analysis is a breach of data privacy).
- copyrighted materials should not be used with AI tools but only original creative artwork.

We support the use of AI where it improves the care and education of children and learners, but we expect all teaching staff to consider if the generated resources are accurate and if the learning outcome is enhanced or diminished by the solution.

We expect staff to remember that generative AI can be: inaccurate, inappropriate or unsafe, biased, taken out of context, taken without permission (intellectual property infringement), out of date or unreliable, low quality

16.1 AI, Deepfakes and Nudification Apps

Our trust recognises that artificial intelligence technologies can be misused to create manipulated, synthetic or AI-generated images, including so-called "nudification" images. These are images which use AI to generate nude or semi-nude depictions of an individual from an ordinary photograph. The creation, possession, sharing or viewing of such imagery involving children or members of the school community may constitute child-on-child abuse, sexual harassment, bullying, intimidation or exploitation and will be treated as a safeguarding concern.

16.2 Key safeguarding risks

16.2.1 Image-based sexual abuse

- A pupil's photograph taken from social media, school websites or messaging apps can be manipulated into a fake nude image.
- The image may then be shared amongst peers, causing significant distress and reputational harm.
- Victims often experience impacts similar to those resulting from real intimate image abuse. [saferinternet.org.uk], [safeguard-hub.org]

16.2.2 Child-on-child abuse

- Children may use AI tools to create sexualised images of classmates.
- Some pupils may wrongly believe that because the image is "not real" it is harmless.
- Schools should treat this as a serious safeguarding concern rather than simply a behaviour issue

16.2.3 Bullying and harassment

- Manipulated images can be used to humiliate, threaten or isolate a victim.
- Images may spread rapidly through messaging groups and social media.
- Victims can experience anxiety, shame, withdrawal from education and reduced wellbeing

16.2.4 Blackmail and coercion

- Fake intimate images may be used to extort money, further images, personal information or compliance with demands.
- Perpetrators may threaten wider distribution if the victim refuses. [saferinternet.org.uk]

16.2.5 Safeguarding investigation challenges

- It can sometimes be difficult to determine whether imagery is genuine or AI-generated.
- Schools focus on procedures that focus on the harm caused rather than debating whether an image is "real".
- Any incidents involving AI-generated intimate imagery will be managed in line with child protection procedures and relevant DfE guidance. Any concerns must be treated as safeguarding concerns and referred to the DSL

17.0 Breaches of the policy

- Any breach of this policy will be fully investigated and may lead to disciplinary action being taken against the employee/s involved in line with the trust's disciplinary policy.
- A breach of this policy leading to breaches of confidentiality, or defamation or damage to the reputation of the trust/school or any illegal act/s that render the trust/school liable to third parties may result in disciplinary action or dismissal.
- Contracted providers of the trust's services must inform the trust immediately if they become aware of any breaches of this policy so that appropriate action can be taken to protect confidential information and limit damage to the reputation of the trust.
- Under the Regulation of Investigatory Powers Act (2000) the trust can exercise the right to monitor the use of the trust's/school's information systems and internet access where it is believed that unauthorised use may be taking place, to ensure compliance with regulatory practices, to ensure standards of service are maintained, to prevent or detect crime, to protect the communications system and to pick up messages if someone is away from school.
- In certain circumstances the trust will be obliged to inform the Local Authority Designated Officer (LADO) and/or police of any activity where there are concerns that it may constitute a safeguarding issue or potentially involve illegal activity.

18.0 How our trust will respond to issues of misuse

- Where a student misuses the trust's IT systems or internet, we will follow the procedures set out in the trust behaviour policy and school protocol. The action taken will depend on the individual circumstances, nature, and seriousness of the specific incident, and will be proportionate.
- Where a staff member misuses the trust's IT systems or the internet or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures. The action taken will depend on the individual circumstances, nature, and seriousness of the specific incident.
- The trust will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.
- Any incidents which result in the unauthorised access, processing or sharing of personal data this will be considered a data breach under the trust data protection and FOI policy and must be notified immediately to the cluster business manager.

19.0 Training

19.1 All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.

- All staff must read and understand Part One of Keeping Children Safe in Education 2026.
- All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

19.2 By way of this training, all staff will be made aware that:

- technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse
- children can abuse their peers online through:
    - Abusive, harassing, and misogynistic messages
    - Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
    - Sharing of abusive images and pornography, to those who don't want to receive such content
    - Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element
- Safety should be the top priority when deciding whether to use generative AI in the classroom

19.3 Annual safeguarding and online safety training will include emerging technologies and AI-related risks, including:

- deepfakes and manipulated media
- AI-generated nude and semi-nude images
- online coercion and image-based abuse
- AI-enabled bullying and harassment
- misinformation and disinformation
- safe and ethical use of generative AI in education
- staff will be supported to recognise indicators of AI-facilitated abuse and understand appropriate safeguarding responses

19.4 Training will also help staff:

- develop better awareness to assist in spotting the signs and symptoms of online abuse
- develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh the risks up
- develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term

19.5 The DSL and deputies will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Board members will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our child protection and safeguarding policy.

20.0 Policy monitoring arrangements

20.1 This policy will be reviewed every year by the executive lead for safeguarding and ratified by the board of trustees. Given the ever-changing nature of technology, we will ensure that this review is supported by ongoing risk assessment which reflects current online safety issues that children face. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

20.2 We will monitor the impact of the policy using:

- logs of reported incidents in the online safety and Filtering and monitoring categories on CPOMS
- internal monitoring data for network activity gathered through filtering and monitoring software
- pupil, staff and family voice

21.0 Review

This policy will be reviewed annually.

Appendix 1: Acceptable use agreement (students and parents/carers)

<table>
<tr><td colspan="4">Beckfoot Trust Acceptable Use Agreement IT Systems and Internet</td></tr>
<tr><td>Name of student:</td><td></td><td>Tutor/reg group:</td><td></td></tr>
<tr><td colspan="4">When using the Trust's IT systems and accessing the internet in trust schools I will:
• Use trust computers, devices, internet access and online services safely, responsibly and for learning purposes.
• Only use technology when a member of staff has given permission or when it is part of a school activity.
• Follow my teacher's instructions when using technology and online resources.
• Keep myself and others safe online by not visiting websites, viewing content or sharing material that may be inappropriate, harmful or upsetting.
• Be kind, respectful and responsible when communicating online and use appropriate language at all times.
• Keep my passwords private and never use another person's account or login details.
• Keep my personal information safe and not share details such as my address, phone number, passwords or other personal information without permission from a parent, carer or member of staff.
• Tell a trusted adult immediately if I see anything online that worries me, upsets me, makes me feel unsafe, or if I am concerned about someone else.
• Be careful when using emails, links, attachments, messages or websites and ask a member of staff if I am unsure.
• Use any personal device brought into school in accordance with school rules and only when permitted by staff.
• Understand that the school monitors the use of its technology and internet services to help keep everyone safe.
• Treat school technology, information and other users with respect at all times.
• Help create a safe and positive online environment for everyone.
• Always use the trust's technology and internet services responsibly and in a way that reflects the trust's values.</td></tr>
<tr><td colspan="2">Signed (Student):</td><td colspan="2">Date:</td></tr>
<tr><td colspan="4">Parent/Carer agreement: I agree that my child can use the school's IT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for Students using the school's IT systems and internet, and for using personal electronic devices in schools and will make sure my child understands these.</td></tr>
<tr><td colspan="2">Signed (Parent/carer):</td><td colspan="2">Date:</td></tr>
</table>

Appendix 2: Acceptable use agreement staff/trust board & LSC members

Beckfoot Trust - Acceptable Use Agreement IT Systems and Internet

When using the trust's IT systems and accessing the internet in trust schools I will:

- Use trust IT systems, devices, accounts and information responsibly, professionally and in accordance with trust safeguarding, cyber security, data protection and acceptable use policies.
- Safeguard children and young people by remaining vigilant to online safety risks, technology-enabled harm, inappropriate content, cyberbullying, exploitation and other safeguarding concerns, and report concerns immediately through school safeguarding procedures.
- Protect trust accounts, systems and data by using strong passwords, multi-factor authentication where provided, and by never sharing passwords or allowing others to use my account.
- Handle personal, confidential and sensitive information in accordance with UK GDPR, the Data Protection Act 2018 and trust policies, ensuring information is accessed, used, shared, retained and disposed of appropriately.
- Remain alert to phishing, cyber-attacks, suspicious emails, messages, links, attachments and websites, and report any concerns promptly through trust procedures.
- Exercise vigilance against fraud, including phishing, impersonation, payment diversion fraud, invoice fraud and requests for sensitive information, and verify unusual requests before taking action.
- Use only trust-approved hardware, software, systems and cloud services, and not install or use unauthorised applications, devices or services.
- Use trust systems professionally and not access, create, store, share or distribute material that is inappropriate, offensive, harmful, discriminatory, illegal or inconsistent with my professional responsibilities.
- Ensure all electronic communications are professional, respectful and appropriate and do not bring the trust into disrepute.
- Maintain appropriate supervision of pupils when using technology and recognise that filtering and monitoring systems support, but do not replace, professional judgement, vigilance and active supervision.
- Immediately report any safeguarding concern, cyber security incident, suspected fraud, data protection breach, system weakness or misuse of trust systems through the appropriate reporting procedures.
- Only use trust IT systems and internet access for legitimate educational or business purposes and in support of my role.
- Understand that the trust monitors the use of its IT systems, devices, networks and internet access to safeguard pupils, protect trust systems and ensure compliance with legal and regulatory requirements.
- Take reasonable steps to keep trust devices, accounts and data secure when working on or off site, including ensuring devices are locked, password protected and information is stored only on approved trust systems.
- Inform the designated safeguarding lead (DSL) immediately if I encounter, or am made aware of, any online content or activity that may place a child at risk of harm.
- Support pupils to use technology safely, responsibly and appropriately, and model good digital, cyber security and data protection practices at all times.
-

*Staff agreement is logged by reading this policy on Every at the start of the academic year or upon induction.

*LSC agreement are in meetings or via Forms as agreed locally.