
the beckmead trust
English Cities
DIGITAL POLICY
nurture
sustain
grow

Policy Level	Trust
Date of Approval	May 2025
Author	Jayesh Parmar
Date of Next Review	May 2026

This policy, as well as covering all items Digital, also covers Online Safety, Acceptable Use and AI (Artificial Intelligence) / LLM (Large Language Models) and Mobile Devices

Contents

Purpose and Scope

The purpose of the Digital Policy is to guide the responsible use of digital technologies within all trust/school and/or residential settings. This policy is also designed to take into account settings outside of the trust/school buildings, incorporating all digital technologies in the Trust or Schools. Specifically any of the devices, applications or platforms that are either owned or controlled by the Trust or Schools.

This policy applies to pupils, staff, and visitors and extends to parents/carers and external stakeholders, such as but not limited to, volunteers, governors, contractors and suppliers/vendors (hereafter referred to as 'individuals'). The term 'Access Credentials' refers to any password, PIN code, token or similar secure item that is used to ensure and maintain the security of a system, account or group which may or may not give permissions and different levels of access.

This policy applies to all information, in whatever form, relating to The Beckmead Trust's business activities worldwide, and to all information handled by The Beckmead Trust relating to other organisations with whom it deals. It also covers all IT and information communications facilities operated by The Beckmead Trust or on its behalf.

Introduction and aims

This policy has 5 distinct sections, but all items within this policy must be considered together:

A) ICT and internet acceptable use
B) Online Safety
C) Artificial Intelligence or Large Language Models
D) Mobile Phones
E) ICT Disaster Recovery

Limitations

- **Evolving Technology:** This policy aims to address current technologies but may not fully cover future technological advancements. Regular reviews will be in place to ensure its continued relevance.
- **Enforcement Challenges:** Consistent enforcement of this policy across all individuals and settings may present practical challenges. Full adherence relies on individual responsibility and reporting.
- **Subjective Interpretation:** Certain aspects of "acceptable use" and "inappropriate content" may be subject to interpretation and professional judgment. The lists defined provide detailed context that can be subject to change based on wider contexts, safeguarding concerns and evolving technologies.
- **External Online Activity:** While this policy governs use of Trust/School ICT facilities, it has limited control over individuals' online activity conducted outside of Trust/School premises or on personal devices.
- **Unforeseen Risks:** Despite comprehensive efforts, this policy may not anticipate all potential risks associated with digital technologies. It is the responsibility of all staff to ensure that the digital conversation for all settings are informed through sharing, dialogue, training and student focussed activities.

Roles and responsibilities

The governing boards (including the trustees)

The relevant governing board (including our trustees) has overall responsibility for monitoring this policy and holding the headteacher, director of education and director of data and technology to account for its implementation.

The governing boards will make sure all staff undergo online safety training as part of child protection and safeguarding training, and ensure staff understand their expectations, roles and responsibilities around filtering and monitoring.

The governing boards will also make sure all staff receive regular online safety updates (via email, e-bulletins and staff meetings), as required and at least annually, to ensure they are continually provided with the relevant skills and knowledge to effectively safeguard children.

The governing boards, via wider safeguarding responsibilities, will meet with appropriate staff to discuss online safety, requirements for training, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

The governing boards should ensure children are taught how to keep themselves and others safe, including keeping safe online.

The governing boards must ensure the trust/school has appropriate filtering and monitoring systems in place on trust/school devices and trust/school networks, and will regularly review their effectiveness. The board will review the DfE's filtering and monitoring standards, and discuss with IT staff and service providers what needs to be done to support the trust/school in meeting the standards, which include:

- Identifying and assigning roles and responsibilities to manage filtering and monitoring systems;
- Reviewing filtering and monitoring provisions at least annually;
- Blocking harmful and inappropriate content without unreasonably impacting teaching and learning;
- Having effective monitoring strategies in place that meet their safeguarding needs.

All governors/trustees will:

- Ensure they have read and that they understand this policy
- Agree and adhere to the terms on acceptable use of the trust/school's ICT systems and the internet (appendix A5)
- Ensure that online safety is a running and interrelated theme while devising and implementing their whole-trust/school or college approach to safeguarding and related policies and/or procedures
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with special educational needs and/or disabilities (SEND). This is because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable

The governing boards will:

- Take overall responsibility for monitoring this policy and holding the headteacher to account for its implementation in line with the trust/school's AI strategy
- Ensure the headteacher and AI lead are appropriately supported to make informed decisions regarding the effective and ethical use of AI in the trust/schools
- Adhere to the guidelines below to protect data when using generative AI tools:
    - Use approved AI tools (see section C5)
    - Recognise that AI tools that are not approved are not supported or within any scope of support from the central IT services team and any staff member in the wider trust
    - Seek advice from the data protection officer / central IT services / AI lead, as appropriate
    - Check whether they are using an open or closed generative AI tool
    - Ensure there is no identifiable information included in what they put into open generative AI tools
    - Acknowledge or reference the use of generative AI in their work

- Fact-check results to make sure the information is accurate

The director of data and technology

The director of data and technology is responsible for ensuring that this policy is up to date, relevant and all headteachers, directors and the executive team have been briefed and show understanding of how to implement the policy in their setting(s) and with their teams.

The headteacher and directors

The headteacher is responsible for ensuring that staff understand this policy, and that it is being followed and implemented consistently throughout their school.

The directors are responsible for ensuring that staff understand this policy, and that it is being followed and implemented consistently throughout their directorate.

The designated safeguarding lead (DSL)

Details of the trust/school's designated safeguarding lead (DSL) and deputy/deputies are set out in our child protection and safeguarding policy, and relevant job descriptions.

The DSL takes lead responsibility for online safety in trust/school, in particular:

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the trust/school
- Working with the headteacher and governing board to review this policy annually and ensure the procedures and implementation are updated and reviewed regularly
- Taking the lead on understanding the filtering and monitoring systems and processes in place on trust/school devices and trust/school networks
- Providing governors with assurance that filtering and monitoring systems are working effectively and reviewed regularly
- Working with the Central IT Services to make sure the appropriate systems and processes are in place
- Working with the headteacher, Central IT Services and other staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the trust/school's child protection policy
- Responding to safeguarding concerns identified by filtering and monitoring
- Ensuring that any online safety incidents are logged (see appendix B5 as a template) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyberbullying are logged and dealt with appropriately in line with the trust/school behaviour policy
- Updating and delivering staff training on online safety (appendix B4 contains a template for self-audit for staff on online safety training needs)
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in trust/school to the headteacher and/or governing board
- Undertaking annual risk assessments that consider and reflect the risks children face
- Providing regular safeguarding and child protection updates, including online safety, to all staff, at least annually, in order to continue to provide them with relevant skills and knowledge to safeguard effectively

This list is not intended to be exhaustive.

Central IT Services

Central IT Services is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems on trust/school devices and trust/school networks, which are reviewed and updated at least annually to assess effectiveness and ensure pupils are kept safe from

potentially harmful and inappropriate content and contact online while at trust/school, including terrorist and extremist material
- Ensuring that the trust/school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the trust/school's ICT systems on a monthly basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged (see appendix B5 template) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the trust/school behaviour policy

This list is not intended to be exhaustive.

All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the trust/school's ICT systems and the internet (appendix A5), and ensuring that pupils follow the trust/school's terms on acceptable use (appendices A3 and A4)
- Knowing that the DSL is responsible for the filtering and monitoring systems and processes, and being aware of how to report any incidents of those systems or processes failing by raising a safeguarding concern with the DSL and/or an IT ticket with central IT services
- Following the correct procedures by getting authorisation from the headteacher and contacting central IT services for authorisation from the director of data and technology if they need to bypass the filtering and monitoring systems for educational purposes
- Working with the DSL to ensure that any online safety incidents are logged (see appendix B5 template) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the trust/school behaviour policy
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline, and maintaining an attitude of 'it could happen here'

This list is not intended to be exhaustive.

Parents/carers

Parents/carers are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the trust/school's ICT systems and internet (appendices A3 and A4)

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

- What are the issues? – UK Safer Internet Centre
- Online safety topics for parents/carers – Childnet
- Parent resource sheet – Childnet

Visitors and members of the community

Visitors and members of the community who use the trust/school's ICT systems or internet will be made aware of this policy and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (appendix A5).

Contacting Central IT Services

Central IT services can be contacted using the ticket desk email address or via the ticket desk portal -

information and guidance on this process can be found on the Beckmead Trust landing pages.

A) ICT and internet acceptable use

A1. Introduction and aims

Information and communications technology (ICT) is integral to how our trust/schools work. It is a critical resource for pupils, staff (including the senior leadership team), governors, volunteers, visitors and any relevant management committees. It supports teaching and learning, and the pastoral and administrative functions of the trust/school.

However, the ICT resources and facilities our trust/school(s) use could also pose risks to data protection, online safety and safeguarding.

This policy aims to:

- Set guidelines and rules on the use of trust/school's ICT resources for staff, pupils, parents/carers and governors
- Establish clear expectations for the way all members of the trust/school community engage with each other online
- Support the trust/school's policies on data protection, online safety and safeguarding
- Prevent disruption that could occur to the trust/school through the misuse, or attempted misuse, of ICT systems
- Support the trust/school in teaching pupils safe and effective internet and ICT use

This policy covers all users of our trust/school's ICT facilities, including governors, staff, pupils, volunteers, contractors and visitors.

Breaches of this policy may be dealt with under the relevant disciplinary/behaviour/staff discipline, or code of conduct policy.

A2. Relevant legislation and guidance

This part of the policy refers to, and complies with, the following legislation and guidance:

- Data Protection Act 2018
- The UK General Data Protection Regulation (UK GDPR) – the EU GDPR was incorporated into UK legislation, with some amendments, by The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2020
- Computer Misuse Act 1990
- Human Rights Act 1998
- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
- Education Act 2011
- Freedom of Information Act 2000
- Education and Inspections Act 2006
- Keeping Children Safe in Education
- Searching, screening and confiscation: advice for trust/schools 2022
- National Cyber Security Centre (NCSC): Cyber Security for trust/schools
- Education and Training (Welfare of Children) Act 2021
- UK Council for Internet Safety (et al.) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- Meeting digital and technology standards in trust/schools and colleges

A3. Definitions

- **ICT facilities:** all facilities, systems and services including, but not limited to, network infrastructure, desktop computers, laptops, tablets, phones, music players or hardware, software, websites, web applications or services, and any device system or service that may become available in the future which is provided as part of the trust/school's ICT service
- **Users:** anyone authorised by the trust/school to use the trust/school's ICT facilities, including governors, staff, pupils, volunteers, contractors and visitors
- **Personal use:** any use or activity not directly related to the users' employment, study or purpose agreed by an authorised user
- **Authorised personnel:** employees authorised by the trust/school to perform systems administration and/or monitoring of the ICT facilities
- **Materials:** files and data created using the trust/school's ICT facilities, including but not limited to documents, photos, audio, video, printed output, web pages, social networking sites and blogs

See Appendix A6 for a glossary of cybersecurity terminology.

A4. Unacceptable use

The following is considered unacceptable use of the trust/school's ICT facilities. Any breach of this policy may result in disciplinary or behaviour proceedings (see section A4.2 below).

Unacceptable use of the trust/school's ICT facilities includes:

- Using the trust/school's ICT facilities to breach intellectual property rights or copyright
- Using the trust/school's ICT facilities to bully or harass someone else, or to promote unlawful discrimination
- Breaching the trust/school's policies or procedures
- Any illegal conduct, or statements which are deemed to be advocating illegal activity
- Online gambling, inappropriate advertising, phishing and/or financial scams
- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate or harmful
- Consensual and non-consensual sharing of nude and semi-nude images and/or videos and/or livestreams
- Activity which defames or disparages the trust/school, or risks bringing the trust/school into disrepute
- Sharing confidential information about the trust/school, its pupils, or other members of the trust/school community
- Connecting any device to the trust/school's ICT network without approval from authorised personnel
- Setting up any software, applications or web services on the trust/school's network without approval by authorised personnel, or creating or using any programme, tool or item of software designed to interfere with the functioning of the trust/school's ICT facilities, accounts or data
- Registering or using accounts for any trust or school activity (such as via email, software, application or web services) that are not on the trust network and/or approved in writing by the director of data and technology (DDT) as outlined in section A4.1. An example of this may be using a @gmail or @outlook or @yahoo email account for trust or school activities.
- Gaining, or attempting to gain, access to restricted areas of the network, or to any password-protected information, without approval from authorised personnel
- Allowing, encouraging or enabling others to gain (or attempt to gain) unauthorised access to the trust/school's ICT facilities
- Causing intentional damage to the trust/school's ICT facilities
- Removing, deleting or disposing of the trust/school's ICT equipment, systems, programmes or information without permission from authorised personnel
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not permitted by authorised personnel to have access, or without authorisation
- Using inappropriate or offensive language
- Promoting a private business, unless that business is directly related to the trust/school and has been authorised by the headteacher or a member of the trust executive team
- Using websites or mechanisms to bypass the trust/school's filtering or monitoring mechanisms

- Engaging in content or conduct that is radicalised, extremist, racist, antisemitic or discriminatory in any other way
- Leaving equipment and media taken off-site unattended in public places and left in sight in a car or other vehicle
- Not carrying Laptops as hand luggage when travelling
- Accepting reverse charge calls from domestic or International operators, unless it is for business use and has been authorised by the headteacher or relevant director
- Using AI tools and generative chatbots (such as ChatGPT and Google Gemini):
    - During assessments, including internal and external assessments, and coursework
    - To write their homework or class assignments, where AI-generated text or imagery is presented as their own work
    - To generate and create content, responses or information for which it is not made clear that AI was used
    - Further guidance on this area can be found in Section C of this policy

This is not an exhaustive list. The trust/school reserves the right to amend this list at any time. The director of data and technology, headteacher or any other relevant member of staff will use their professional judgement to determine whether any act or behaviour not on the list above is considered unacceptable use of the trust/school's ICT facilities.

A4.1 Exceptions from unacceptable use

Where the use of trust/school ICT facilities (on the trust/school premises and/or remotely) is required for a purpose that would otherwise be considered an unacceptable use, exemptions to the policy may be granted at the director of data and technology's (DDT) discretion. The Trust IT ticketing service can be used to make a request and the heading "Exceptions from unacceptable use" must be in the subject line to ensure that the request is swiftly forwarded to the DDT.

A4.1.1 Using AI (Artificial Intelligence) and LLM (Large Language Models)

The use of AI and LLM tools, such as Gemini, etc., is permitted for business purposes within The Beckmead Trust, subject to the following conditions which can be amended at any time and are subject to the full details regarding AI in section C of this policy:

- **Data Privacy:** Any confidential or sensitive information pertaining to The Beckmead Trust or its stakeholders must NOT be input into AI/LLM tools.
- **Output Ownership:** All outputs generated by AI/LLM tools are the property of The Beckmead Trust.
- **Accuracy and Verification:** Information obtained from AI/LLM tools should be carefully evaluated for accuracy and should not be considered a replacement for professional judgment or expertise.
- **Bias and Discrimination:** Users must be aware of the potential for bias in AI/LLM-generated content and take steps to mitigate it.
- **Transparency:** When using AI/LLM tools in the creation of content, it should be clearly indicated that the content was generated or assisted by AI.
- **Security:** Users must adhere to The Beckmead Trust's security policies when using AI/LLM tools.

Individuals must not:

- Use AI/LLM tools for any purpose that violates The Beckmead Trust's policies or values.
- Use AI/LLM tools to create content that is harmful, unsafe, biased, or unfair.
- Attempt to reverse engineer or manipulate AI/LLM tools.

The Beckmead Trust reserves the right to monitor the use of AI/LLM tools and to take appropriate action in cases of misuse.

A4.2 Sanctions

Pupils and staff who engage in any of the unacceptable activities listed above may face disciplinary action in line with the trust/school's policies on disciplinary/behaviour/staff discipline, or code of conduct.

Specific and special sanctions and restrictions for unacceptable ICT use can be imposed at the discretion of the director of data and technology.

Copies of the relevant policies can be found on the Beckmead Trust website.

A5. Staff (including governors, volunteers, and contractors)

A5.1 Access to trust/school ICT facilities and materials

The trust/school's central IT services (under the data and technology directorate) manage access to the trust/school's ICT facilities and materials for trust/school staff. That includes, but is not limited to:

- Computers, tablets, mobile phones and other devices
- Access permissions for certain programmes or files

Staff will be provided with unique login/account information and passwords that they must use when accessing the trust/school's ICT facilities.

Staff who have access to files that they are not authorised to view or edit, or who need their access permissions updated or changed, **must** contact the central IT service by raising a ticket. Further information can be found on the Beckmead Trust Staff Landing pages.

A5.1.1 Use of communications - phones and email (including virtual meetings/calls, chat and spaces or equivalent)

The trust/school provides each member of staff with an email address to use. The system also enables staff to conduct virtual meetings/calls and use the chat and spaces functionality via their email account. *The term 'email' will be extended to also cover the use of virtual meetings/calls, chat and spaces with any relevant item listed below applying to the relevant matching technology/system under the 'email' heading.*

This email account should be used for work purposes only. Staff should enable multi-factor authentication on their email account(s) wherever possible.

All work-related business should be conducted using the email address the trust/school has provided.

Staff must not share their personal email addresses with parents/carers and pupils. Staff must not send any work-related materials using their personal email account.

Staff must take care with the content of all email messages. Incorrect or improper statements can cause claims for discrimination, harassment, defamation, breach of confidentiality or breach of contract.

Email messages are required to be disclosed in legal proceedings or in response to requests from individuals under the Data Protection Act 2018 in the same way as paper documents. Deletion from a user's inbox does not mean that an email cannot be recovered for the purposes of disclosure. All email messages should be treated as potentially retrievable.

Staff must take extra care when sending sensitive or confidential information by email. Any attachments containing sensitive or confidential information should be encrypted so that the information is only accessible by the intended recipient.

If staff receive an email in error, the sender should be informed and the email deleted. If the email contains sensitive or confidential information, the user must not make use of that information or disclose that information.

If staff send an email in error that contains the personal information of another person, they must inform the central IT services immediately and follow our data breach procedure.

Staff must not give their personal phone number(s) to parents/carers or pupils. Staff must use phones provided by the trust/school to conduct all work-related business.

Trust/school phones must not be used for personal matters.

Staff who are provided with mobile phones as equipment for their role must abide by the same rules for ICT acceptable use as set out in section A4.

Some of the trust/school systems have the functionality to record incoming and outgoing meetings/phone conversations.

If you record meetings/calls, participants/callers **must** be made aware that the conversation is being recorded and the reasons for doing so.

Explain when you record meetings/phone conversations and why. For instance:

- "All calls to the trust/school office are recorded to aid administrators"
- "Calls are recorded for use in staff training"
- "The recording is to be used as a record of the event"

A5.2 Personal use

Staff are permitted to occasionally use trust/school ICT facilities for personal use, subject to certain conditions set out below. This permission must not be overused or abused. Central IT services may withdraw or restrict this permission at any time and at their discretion.

Personal use is permitted provided that such use:

- Does not take place during school hours (usually 8am to 4pm on weekdays)
- Does not constitute 'unacceptable use', as defined in section A4
- Takes place when no pupils are present
- Does not interfere with their jobs, or prevent other staff or pupils from using the facilities for work or educational purposes

Staff may not use the trust/school's ICT facilities to store personal, non-work-related information or materials (such as music, videos or photos).

Staff should be aware that use of the trust/school's ICT facilities for personal use may put personal communications within the scope of the trust/school's ICT monitoring activities (see section A5.5). Where breaches of this policy are found, disciplinary action may be taken.

Staff are also permitted to use their personal devices (such as mobile phones or tablets) in line with the trust/school's mobile phones section of this policy.

Staff should be aware that personal use of ICT (even when not using trust/school ICT facilities) can impact their employment by, for instance, putting personal details in the public domain, where pupils and parents/carers could see them.

Staff should take care to follow the trust/school's guidelines on use of social media (see appendix A1) and use of 'email' (see section 5.1.1) to protect themselves online and avoid compromising their professional integrity.

A5.2.1 Personal social media accounts

Staff should ensure that their use of social media, either for work or personal purposes, is appropriate at all times.

The trust/school has guidelines for staff on appropriate security settings for Facebook accounts (see appendix A1).

A5.3 Remote access

We allow staff to access the trust/school's ICT facilities and materials remotely. They should use the appropriate methods as outlined when given access remotely. The details of any remote access given must be kept secure.

Staff accessing the trust/school's ICT facilities and materials remotely must abide by the same rules as those accessing the facilities and materials on site. Staff must be particularly vigilant if they use the trust/school's ICT facilities outside the trust/school and must take such precautions as the central IT services may require against importing viruses or compromising system security.

Our ICT facilities contain information which is confidential and/or subject to data protection legislation. Such information must be treated with extreme care and in accordance with our data protection policy.

The trust/school data protection policy can be found on the Beckmead Trust website.

A5.4 Trust/school social media accounts

The trust/school has official social media accounts, managed by the comms team centrally. Staff members who have not been authorised to manage, or post to, the account, must not access, or attempt to access, the account.

The trust/school has guidelines for what may and must not be posted on its social media accounts. Those who are authorised to manage, or post to, the account must make sure they abide by these guidelines at all times.

A5.5 Monitoring and filtering of the trust/school network and use of ICT facilities

To safeguard and promote the welfare of children and provide them with a safe environment to learn, the trust/school reserves the right to filter and monitor the use of its ICT facilities and network. This includes, but is not limited to, the filtering and monitoring of:

- Internet sites visited
- Bandwidth usage
- Email accounts
- Telephone calls
- User activity/access logs
- Any other electronic communications

Only authorised ICT personnel may filter, inspect, monitor, intercept, assess, record and disclose the above, to the extent permitted by law. We serve a diverse and wide range of students and parents/carers - so the way we inform parents/carers of filtering and monitoring is school-based and school-organised (please contact the school directly for further information - the school office email can be found on the Beckmead Trust website). The systems used for monitoring and filtering range from hardware and software firewalls to classroom management and safeguarding monitoring tools and the tools built into the Google, Microsoft and Apple systems and their subsidiary management platforms. There will also be other systems that are used to monitor and filter beyond this and specific details of these can be obtained on request by contacting the school.

The trust/school monitors ICT use in order to:

- Maintain safeguarding protocols and procedures
- Support teaching and learning
- Obtain information related to trust/school business
- Investigate compliance with trust/school policies, procedures and standards
- Ensure effective trust/school and ICT operation
- Conduct training or quality control exercises
- Prevent or detect crime
- Comply with a subject access request, Freedom of Information Act request, or any other legal obligation

Our governing board is responsible for making sure that:

- The trust/school meets the DfE's filtering and monitoring standards
- Appropriate filtering and monitoring systems are in place
- Staff are aware of those systems and trained in their related roles and responsibilities
    - For the leadership team and relevant staff, this will include how to manage the processes and systems effectively and how to escalate concerns
- It regularly reviews the effectiveness of the trust/school's monitoring and filtering systems

The trust/school's designated safeguarding lead (DSL) will take lead responsibility for understanding the filtering and monitoring systems and processes in place.

Where appropriate, staff may raise concerns about monitored activity with the trust/school's DSL and central IT services, as appropriate.

A5.6 Clear Desk and Clear Screen Policy

In order to reduce the risk of unauthorised access or loss of information, The Beckmead Trust enforces a clear desk and screen policy as follows:

- Personal or confidential business information must be protected using security features provided for example by secure print on printers.
- Computers must be logged off/locked or protected with a screen-locking mechanism controlled by Access Credentials when unattended.
- Care must be taken to not leave confidential material on printers or photocopiers.
- All business-related printed matter must be disposed of using confidential waste bins or shredders.

A5.7 Actions upon Termination of Contract

All Beckmead Trust equipment and data, for example laptops and mobile devices including telephones, smartphones, USB memory devices and CDs/DVDs, must be returned to The Beckmead Trust at termination of contract.

All Beckmead Trust data or intellectual property developed or gained during the period of employment remains the property of The Beckmead Trust and must not be retained beyond termination or reused for any other purpose.

A5.8 Device Asset Responsibility

All Beckmead Trust equipment, for example laptops and mobile devices including telephones, smartphones, as well cameras and other items of technology, are the responsibility of the staff member to whom the device is signed out to.

All staff must ensure that they look after any equipment on or off school/trust premises - regardless of whether it is signed in/out to them - they must report any issues with equipment immediately either via their line manager/headteacher or by using the ticketing system (guidance can be found on the trust landing pages on how to log a ticket).

It is also important that staff are vigilant about equipment that is movable that is left unattended and/or potentially at risk of being taken. Staff have to a duty to ensure that they collect and report any equipment that they find unattended and/or may be at risk and return it to the person to whom the equipment is signed out or to the headteacher - some examples of this are below (but the list is not exhaustive) - The equipment:

- Is unattended in an open classroom, staff room/space, canteen/hall, reception area, entrance area
- Has been found in the possession of a parent/carer, visitor, student or other non-staff member and should not be in their possession
- Is in an unlocked vehicle
- Is in view in a locked vehicle
- Is left unlocked from a data access/login point of view

It is the responsibility of staff member who is taking a device from another staff member, the school or trust to use the signing in/out form provided on the schools landing page - under the page “forms” (this can be found via the trust landing page).

Student laptops will be assigned to the relevant staff member who is responsible for the subject, room, space or group usually at the beginning of a term or academic year - it is the responsibility of that staff member to ensure that these devices locations are always known, and that they are looked after, in working order and assigned to the relevant students. All student laptops must be assigned to be responsible by a staff member and it is the headteachers responsibility to ensure that the staff teams are clear on who is responsible for what student devices.

A6. Pupils

A6.1 Access to ICT facilities

- Pupils have access to devices in their classrooms
- At the discretion of the headteacher pupils may also be able to access a trust/school device at home
- Computers and equipment in any of the trust/school's classrooms (including the ICT suite) are available to pupils only under the supervision of staff
- Specialist ICT equipment, such as that used for creative, film, graphic, music, or design and technology, must only be used under the supervision of staff
- Pupils will be provided with an account linked to the trust/school's virtual learning environment, which they can access from any device by using the following URL: *https://sites.google.com/beckmeadtrust.org/students/home*

A6.2 Search and deletion

Under the Education Act 2011, the headteacher, and any member of staff authorised to do so by the headteacher, can search pupils and confiscate their mobile phones, computers or other devices that the authorised staff member has reasonable grounds for suspecting:

- Poses a risk to staff or pupils, **and/or**
- Is identified in the trust/school rules as a banned item for which a search can be carried out, **and/or**
- Is evidence in relation to an offence

This includes, but is not limited to:

- Pornography*
- Abusive messages, images or videos*
- Indecent images of children*
- Evidence of suspected criminal behaviour (such as threats of violence or assault)*

Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:

- Make an assessment of how urgent the search is, and consider the risk to other pupils and staff. If the search is not urgent, they will seek advice from the headteacher or the director of education or the director of data and technology
- Explain to the pupil why they are being searched, and how and where the search will happen, and give them the opportunity to ask questions about it
- Seek the pupil's co-operation (if the pupil refuses to cooperate, proceed according to your behaviour policy and guidance from the headteacher or relevant senior leader that is the behaviour lead)

The authorised staff member should:

- Inform the DSL (or deputy) of any searching incidents where they had reasonable grounds to suspect a pupil was in possession of a banned item. An example of banned digital items are listed above with a *. The Weapons policy also has a list of other banned items (this can be found on the Beckmead Trust website).
- Involve the DSL (or deputy) without delay if they believe that a search has revealed a safeguarding risk

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on a device that they have confiscated where they believe there is a 'good reason' to do so.

When deciding whether there is a 'good reason' to examine data or files on a device, the staff member should only do so if they reasonably suspect that the data has been, or could be, used to:

- Cause harm, **and/or**
- Undermine the safe environment of the trust/school or disrupt teaching, **and/or**
- Commit an offence

If inappropriate material is found on the device, it is up to the staff member along with the DSL / headteacher / other member of the senior leadership team (this decision and action should not be made alone) to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding whether there is a good reason to erase data or files from a device, staff members will consider whether the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as is reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to any person, **and/or**
- The pupil and/or the parent refuses to delete the material themselves

If a staff member **suspects** a device **may** contain an indecent image of a child (also known as a nude or semi-nude image), they will:

- **Not** view the image
- **Not** copy, print, share, store or save the image
- Confiscate the device and report the incident to the DSL (or deputy) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on searching, screening and confiscation and the UK Council for Internet Safety (UKCIS) et al.'s guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

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

- The DfE's latest guidance on searching, screening and confiscation
- UKCIS et al.'s guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- Our behaviour policy / weapons policy (available on the Beckmead Trust website)

Any complaints about searching for, or deleting, inappropriate images or files on pupils' devices will be dealt with through the trust/school complaints procedure.

A6.3 Unacceptable use of ICT and the internet outside of trust/school

The trust/school will sanction pupils, in line with the behaviour policy, if a pupil engages in any of the following **at any time** (even if they are not on trust/school premises):

- Using ICT or the internet to breach intellectual property rights or copyright
- Using ICT or the internet to bully or harass someone else, or to promote unlawful discrimination
- Breaching the trust/school's policies or procedures
- Any illegal conduct, or making statements which are deemed to be advocating illegal activity
- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate
- Consensual or non-consensual sharing of nude and semi-nude images and/or videos and/or livestreams (also known as sexting or youth produced sexual imagery)
- Activity which defames or disparages the trust/school, or risks bringing the trust/school into disrepute
- Sharing confidential information about the trust/school, other pupils, or other members of the trust/school community
- Gaining or attempting to gain access to restricted areas of the network, or to any password-protected information, without approval from authorised personnel
- Allowing, encouraging, or enabling others to gain (or attempt to gain) unauthorised access to the trust/school's ICT facilities
- Causing intentional damage to the trust/school's ICT facilities or materials
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user and/or those they share it with are not supposed to have access, or without authorisation
- Using inappropriate or offensive language

- Using AI tools unreasonably, irresponsibly or to cause harm or negative impact on any Beckmead Trust stakeholder (particularly other students)

A7. Parents/carers

A7.1 Access to ICT facilities and materials

Parents/carers do not have access to the trust/school's ICT facilities as a matter of course.

However, parents/carers working for, or with, the trust/school in an official capacity (for instance, as a volunteer or as a member of the PTA) may be granted an appropriate level of access, or be permitted to use the trust/school's facilities at the headteacher's discretion.

Where parents/carers are granted access in this way, they must abide by this policy as it applies to staff.

A7.2 Communicating with or about the trust/school online

We believe it is important to model for pupils, and help them learn how to communicate respectfully with, and about, others online.

Parents/carers play a vital role in helping model this behaviour for their children, especially when communicating with the trust/school through our website and social media channels.

We ask parents/carers to sign the agreement in appendix A2.

A7.3 Communicating with parents/carers about pupil activity

When we ask pupils to use websites or engage in online activity, these are all done via our monitoring and filtering solutions.

In relation to home or remote learning, staff will let parents/carers know which (if any) person or people from the trust/school pupils will be interacting with online, including the purpose of the interaction.

Parents/carers may seek any support and advice from the trust/school to ensure a safe online environment is established for their child.

Please contact the school office (details can be found on the Beckmead Trust website) for further information on any of the above.

A8. Data security

The trust/school is responsible for making sure it has the appropriate level of security protection and procedures in place to safeguard its systems, staff and learners. It therefore takes steps to protect the security of its computing resources, data and user accounts. The effectiveness of these procedures is reviewed periodically to keep up with evolving cyber crime technologies.

Staff, pupils, parents/carers and others who use the trust/school's ICT facilities should use safe computing practices at all times. We aim to meet the cyber security standards recommended by the Department for Education's guidance on digital and technology standards in trust/schools and colleges, including the use of:

- Firewalls
- Security features
- User authentication and multi-factor authentication
- Anti-malware software

A8.1 Passwords

All users of the trust/school's ICT facilities should set strong passwords for their accounts and keep these passwords secure. Please log a ticket with the central IT services if you wish to find out what the requirements are.

Users are responsible for the security of their passwords and accounts, and for setting permissions for accounts and files they control.

Staff or students who disclose account or password information may face disciplinary action. Parents, visitors or volunteers who disclose account or password information may have their access rights revoked.

All staff will use the password manager required by central IT services to help them store their passwords securely (details of this can be found on induction/yearly training/trust landing pages). Relevant staff will have access to the generated passwords for pupils via a secure document and will need to keep these secure and not share this document or its contents. The relevant staff member will be responsible for sharing/distributing passwords in case pupils lose or forget their passwords.

On occasion passwords will be required to be changed (this will usually be done with plenty of notice) - guidance, notice and information will be provided through the schools senior leadership team or relevant central directors.

A8.2 Software updates, firewalls and anti-virus software

All of the trust/school's ICT devices that support software updates, security updates and anti-virus products will have these installed, and be configured to perform such updates regularly or automatically.

Users must not circumvent or make any attempt to circumvent the administrative, physical and technical safeguards we implement and maintain to protect personal data and the trust/school's ICT facilities.

Any personal devices using the trust/school's network must all be configured in this way.

A8.3 Data protection

All personal data must be processed and stored in line with data protection regulations and the trust/school's data protection policy.

The data protection policy can be found on the Beckmead Trust website.

A8.4 Access to facilities and materials

All users of the trust/school's ICT facilities will have clearly defined access rights to trust/school systems, files and devices.

These access rights are managed via the HR process and a user's job role and responsibilities.

Users should not access, or attempt to access, systems, files or devices to which they have not been granted access. If access is provided in error, or if something a user should not have access to is shared with them, they **must** alert central IT services immediately.

Users should always log out of systems and lock their equipment when they are not in use to avoid any unauthorised access. Equipment and systems should always be logged out of and shut down completely at the end of each working day.

A8.5 Encryption

The trust/school ensures its devices and systems have an appropriate level of encryption.

Trust/school staff may only use personal devices (including computers and USB drives) to access trust/school data, work remotely, or take personal data (such as pupil information) out of trust/school if they have been specifically authorised to do so by the headteacher or director of data and technology.

Use of such personal devices will only be authorised if the devices have appropriate levels of security and encryption, as defined by central IT services.

A9. Protection from cyber attacks

Please see the glossary (appendix A6) to help you to understand cyber security terminology.

The trust/school will:

- Work with governors and the IT department to make sure cyber security is given the time and resources it needs to make the trust/school secure
- Provide annual training for staff (and include this training in any induction for new starters, if they join outside of the trust/school's annual training window) on the basics of cyber security, including how to:

- Check the sender's address in an email (also recognising unusual requests)
- Respond to a request for bank details, personal information or login details
- Verify requests for payments or changes to information

- Make sure staff are aware of its procedures for reporting and responding to cyber security incidents
- Investigate whether our IT software needs updating or replacing to be more secure
- Not engage in ransom requests from ransomware attacks, as this would not guarantee recovery of data
- Put controls in place that are:
  - **Proportionate**: the trust/school will verify this using a third-party audit (such as Cyber Essentials or 360 degree safe) annually, to objectively test that what it has in place is effective
  - **Multi-layered**: everyone will be clear on what to look out for to keep our systems safe
  - **Up to date:** with a system in place to monitor when the trust/school needs to update its software
  - **Regularly reviewed and tested**: to make sure the systems are as effective and secure as they can be
- Backup of critical data will be conducted at least daily (with expected higher frequency automatic backups) with storage of these backups on cloud-based backup systems that aren't connected to the trust/school network.
- Delegate specific responsibility for maintaining the security of our management information system (MIS) to our cloud-based provider with oversight from central IT services.
- Make sure staff:
  - Dial into our network using a virtual private network (VPN) where this is appropriate
  - Enable multi-factor authentication in all places where it is possible, on things like trust/school email accounts, software and web-based applications
  - Store passwords securely using the password manager advised by the central IT team
- Make sure ICT staff conduct regular access reviews to make sure each user in the trust/school has the right level of permissions and admin rights
- Have a firewall in place, ensure that is switched on and in working order
- Check that its supply chain is secure, for example by asking suppliers about how secure their business practices are and checking if they have the Cyber Essentials certification
- Develop, review and test an incident response plan with the IT department including, for example, how the trust/school will communicate with everyone if communications go down, who will be contacted and when, and who will notify Action Fraud of the incident. This plan will be reviewed and tested every 6 months and after a significant event has occurred, using the NCSC's 'Exercise in a Box'
- Work with all relevant partners including the DfE and Local Authorities to see what it can offer the trust/school regarding cyber security, such as advice on which service providers to use or assistance with procurement

A10. Internet access

The trust/school's wireless internet connection is secure.

Filters are in place at all times across all trust/school broadband internet access

Please note - Filters aren't foolproof. Staff **must** contact central IT services if you have details of inappropriate sites that have not been filtered (or appropriate sites that have been filtered in error).

A10.1 Pupils

Access to WiFi is available on all trust/school devices

- Filtering for pupils is of a higher order than staff filtering
  - Students should not use staff machines to access the internet unless it is for a specific use case and authorised by the headteacher
- Internet and WiFi is available to students to use and limited to educational purposes
- Internet and WiFi access in residential settings is different to school access as below:
  - Pupils can request access via their residential staff teams

- Pupils can access WiFi on their device in line with the residential provisions protocols and procedures (these can be found on the Beckmead Trust website under the relevant provisions protocols and procedures documentation)

A10.2 Parents/carers and visitors

Parents/carers and visitors to the trust/school will be permitted to use the trust/school's **"guest"** WiFi only for the following purposes:

- Parents/carers are working with the trust/school in an official capacity (e.g. as a volunteer or as a member of the PTA)
- Visitors need to access the trust/school's WiFi in order to fulfil the purpose of their visit (for instance, to access materials stored on personal devices as part of a presentation or lesson plan)
- There is a residential visit from a parent/carer or other family member in the residential setting where having access to WiFi would promote, enable and develop relationships or support for the young person in their residential place
- Parent/carer supervision is important and particularly relevant when a student is using a device outside of the school setting. This is where filtering and monitoring is based on the personal home connections and systems that are not managed by the schools/trust and therefore require parent/carers additional support and vigilance to ensure safeguarding is maintained

Staff must not give the WiFi password to anyone who is not authorised to have it. Doing so could result in disciplinary action.

The above is in effect unless specific authorisation is granted by the director of data and technology for additional or a different level of access to the internet or WiFi on a case-by-case basis.

B) Online safety policy

B1. Aims

Our trust/school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Identify and support groups of pupils that are potentially at greater risk of harm online than others
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole trust/school community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones')
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

The 4 key categories of risk

Our approach to online safety is based on addressing the following categories of risk:

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

B2. Legislation and guidance

This policy is based on the Department for Education's (DfE's) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for trust/schools on:

- Teaching online safety in trust/schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and trust/school staff
- Relationships and sex education – remove if not applicable, see section B4
- Searching, screening and confiscation

It also refers to the DfE's guidance on protecting children from radicalisation.

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 pupils' electronic devices where they believe there is a 'good reason' to do so.

The policy also takes into account the National Curriculum computing programmes of study.

This policy complies with our funding agreement and articles of association.

B3. Roles and responsibilities

Details can be found in the Roles and responsibilities section of this policy

B4. Educating pupils about online safety

The trust/schools support a wide range of students with varying needs who are working at different levels in relation to what is commonly agreed to be a typical national curriculum key stage level. This means a student may be in Key Stage 2 because of their age but they may be working at Key Stage 1 because of their particular needs. So the guidance below does not outline the students position by age but by the level they are currently working at - this is personalised to each pupil and agreed at school level.

Pupils will be taught about online safety **fundementals** as part of the curriculum:

All trust/schools have to teach:

- Relationships education and health education in primary trust/schools
- Relationships and sex education and health education in secondary trust/schools

Pupils working at a level equivalent to **Key Stage (KS) 1**, 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

Pupils working at a level equivalent to **Key Stage (KS) 2** 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
- Be discerning in evaluating digital content

By the **end of students working at a Key Stage (KS) 2 level**, pupils will know:

- That people sometimes behave differently online, including by pretending to be someone they are not
- That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online, including when we are anonymous
- The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them
- How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met
- How information and data is shared and used online
- What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context)
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know
- The benefits of rationing time spent online, the risks of excessive time spent on electronic devices and the impact of positive and negative content online on their own and others' mental and physical wellbeing
- How to consider the effect of their online actions on others and know how to recognise and display respectful behaviour online and the importance of keeping personal information private
- Where and how to report concerns and get support with issues online

Pupils working at a level equivalent to **Key Stage (KS) 3**, 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

Pupils working at a level equivalent to **Key Stage (KS) 4** 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

By the **end of students working at a Key Stage (KS) 4 level**, pupils will know:

- Their rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online

- About online risks, including that any material someone provides to another has the potential to be shared online and the difficulty of removing potentially compromising material placed online
- Not to provide material to others that they would not want shared further and not to share personal material that is sent to them
- What to do and where to get support to report material or manage issues online
- The impact of viewing harmful content
- That specifically sexually explicit material (e.g. pornography) presents a distorted picture of sexual behaviours, can damage the way people see themselves in relation to others, and negatively affect how they behave towards sexual partners
- That sharing and viewing indecent images of children (including those created by children) is a criminal offence that carries severe penalties including jail
- How information and data is generated, collected, shared and used online
- How to identify harmful behaviours online (including bullying, abuse or harassment) and how to report, or find support, if they have been affected by those behaviours
- How people can actively communicate and recognise consent from others, including sexual consent, and how and when consent can be withdrawn (in all contexts, including online)

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

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

B5. Educating parents/carers about online safety

The trust/school will raise parents/carers' awareness of internet safety in letters or other communications home, and in information via our website or virtual learning environment (VLE). This policy will also be shared with parents/carers.

Online safety will also be covered during parents' evenings.

The trust/school will let parents/carers know:

- What systems the trust/school uses to filter and monitor online use
- For home/remote learning - additional information will be provided on what their children are being asked to do online, including the sites they will be asked to access and who from the trust/school (if anyone) their child will be interacting with online

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.

B6. Cyber-bullying

B6.1 Definition

Cyber-bullying occurs online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of 1 person or group by another person or group, where the relationship involves an imbalance of power. (See also the trust/school behaviour policy.)

B6.2 Preventing and addressing cyber-bullying

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

The trust/school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Teachers will discuss cyber-bullying with their tutor groups.

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, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training (see section B11 for more detail).

The trust/school also sends information/leaflets on cyber-bullying to parents/carers so 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 trust/school will follow the processes set out in the trust/school behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the trust/school will use all reasonable endeavours to ensure the incident is contained.

The DSL will report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

B6.3 Artificial intelligence (AI)

Generative artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Gemini.

The Beckmead Trust recognises that AI has many uses to help pupils learn, but may also have the potential to be used to bully others. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real. This includes deepfake pornography: pornographic content created using AI to include someone's likeness.

The Beckmead Trust will treat any use of AI to bully pupils very seriously, in line with our behaviour policy.

Staff should be aware of the risks of using AI tools whilst they are still being developed and should carry out a risk assessment where new AI tools are being used by the trust/school, and where existing AI tools are used in cases which may pose a risk to all individuals that may be affected by it, including, but not limited to, pupils and staff.

Any use of Artificial Intelligence should be carried out in accordance with this policy and in particular section C (Use of artificial intelligence).

B7. Acceptable use of the internet in trust/school

All pupils, parents/carers, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the trust/school's ICT systems and the internet (appendices A2 to A5). Visitors will be expected to read and agree to the trust/school's terms on acceptable use if relevant.

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

We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they follow the above and restrict access through filtering systems where appropriate.

More information is set out in the acceptable use agreements in appendices A2 to A5.

B8. Pupils using mobile devices in trust/school

Please refer to section D5 for further information on this area

B9. Staff using work devices outside trust/school

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping the device password-protected – strong passwords can be made up of three random words, in combination with numbers and special characters if required, or generated by a password manager. Further details can be requested from central IT services via a ticket
- Ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends
- Installing anti-virus and anti-spyware software
- Keeping operating systems up to date by always installing the latest updates

Staff members must not use the device in any way that would violate the trust/school's terms of acceptable use, as set out in appendix A5.

Work devices must be used for work activities with a small scope for personal use as outlined in A5.2

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

B10. How the trust/school will respond to issues of misuse

Where a pupil misuses the trust/school's ICT systems or internet, we will follow the procedures set out in this policy and (but not limited to) our behaviour policy. 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/school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with this policy and (but not limited to) the staff code of conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The trust/school will consider whether incidents that involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

B11. Training

B11.1 Staff, governors and volunteers

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 members will receive refresher training at least once each academic year as part of safeguarding training, and relevant updates as required (for example through emails, e-bulletins and staff meetings).

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, threatening, 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
- 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 up the risks
    - Develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term

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.

Governors 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.

B11.2 Pupils

All pupils will receive age-appropriate and working level appropriate training on safe internet use, including:

- Methods that hackers use to trick people into disclosing personal information
- Password security
- Social engineering
- The risks of removable storage devices (e.g. USBs)
- Multi-factor authentication
- How to report a cyber incident or attack
- How to report a personal data breach

Pupils will also receive age-appropriate and working level appropriate training on safeguarding issues such as cyberbullying and the risks of online radicalisation.

B11.3 Digital Safety Resources

To support our commitment to digital safety, appendix B2 compiles a selection of recommended resources. These materials are designed to educate and empower our school community with the knowledge and skills necessary to navigate the online world safely and responsibly, covering topics relevant to all age groups.

There is also appendix B3 that holds any posters that are relevant and appropriate to share.

B12. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety - they **must** use the trust safeguarding system for the school.

An additional incident report log template can be found in appendix B5 - if there are any issues logging due to system downtime or another technical or training issue.

An Annual risk assessment - considering and reflecting on the risks pupils face online will be carried out every year and can be found in appendix B1. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

C) Use of artificial intelligence (AI) policy

C1. Aims and scope

The Beckmead Trust understands the valuable potential that artificial intelligence (AI), including generative AI, holds for trust/schools. For example, it can be used to enhance pedagogical methods, customise learning experiences and progress educational innovation.

We are also aware of the risks posed by AI, including data protection breaches, copyright issues, ethical implications, safeguarding and compliance with wider legal obligations.

Therefore, the aim of this policy is to establish guidelines for the ethical, secure and responsible use of AI technologies across our whole trust/school community.

This policy covers the use of AI tools by trust/school staff, governors and pupils. This includes generative chatbots like ChatGPT and Google Gemini (please note, this list is not exhaustive).

This policy aims to:

- Support the use of AI to enhance teaching and learning
- Support staff to explore AI solutions to improve efficiency and reduce workload
- Prepare staff, governors and pupils for a future in which AI technology will be an integral part
- Promote equity in education by using AI to address learning gaps and provide personalised support
- Ensure that AI technologies are used ethically and responsibly by all staff, governors and pupils
- Protect the privacy and personal data of staff, governors and pupils in compliance with the UK GDPR

C1.1 Definitions

This policy refers to both 'open' and 'closed' generative AI tools. These are defined as follows:

- **Open generative AI tools** are accessible and modifiable by anyone. They may store, share or learn from the information entered into them, including personal or sensitive information
- **Closed generative AI tools** are generally more secure, as external parties cannot access the data you input

C2. Legislation

This policy reflects good practice guidelines/recommendations in the following publications:

- AI regulation white paper, published by the Department for Science, Innovation and Technology, and the Office for Artificial Intelligence
- Generative artificial intelligence (AI) and data protection in trust/schools, published by the Department for Education (DfE)
- Generative AI: product safety expectations - GOV.UK, published by the Department for Education (DfE)

This policy also meets the requirements of the:

- UK General Data Protection Regulation (UK GDPR) – the EU GDPR was incorporated into UK legislation, with some amendments, by The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2020
- Data Protection Act 2018 (DPA 2018)

C3. Regulatory principles

We follow the 5 principles set out in the AI regulation white paper.

REGULATORY PRINCIPLE	WE WILL …
Safety, security and robustness	• Ensure that AI solutions are secure and safe for users and protect users' data • Ensure we can identify and rectify bias or error • Anticipate threats such as hacking
Appropriate transparency and explainability	• Be transparent about our use of AI, and make sure we understand the suggestions it makes
Fairness	• Only use AI solutions that are ethically appropriate, equitable and free from prejudice – in particular, we will fully consider any bias relating to small groups and protected characteristics before using AI, monitor bias closely and correct problems where appropriate
Accountability and governance	• Ensure that the governing board and staff have clear roles and responsibilities in relation to the monitoring, evaluation, maintenance and use of AI
Contestability and redress	• Make sure that staff are empowered to correct and overrule AI suggestions – decisions should be made by the user of AI, not the technology • Allow and respond appropriately to concerns and complaints where AI may have caused error resulting in adverse consequences or unfair treatment

C4. Roles and responsibilities

C4.0 AI lead

The Trust generative AI lead is the director of data and technology. They are responsible for the strategic leadership of AI use in the trust.

The headteacher is responsible for the day-to-day ownership and management of AI use in their school.

C4.1 Governing boards

Details can be found in the Roles and responsibilities section of this policy

C4.2 Strategic and Operational Roles

C4.2.1 Director of data and technology

The director of data and technology will:

- Take responsibility for the strategic leadership of AI use in the trust
- Liaise with the data protection officer (DPO) to ensure that the use of AI is in accordance with data protection legislation
- Review and update this AI policy as appropriate, and at least annually

- Sign off on approved uses of AI, or new AI tools, taking into account advice from the DPO and data protection impact assessments

C4.2.2 Headteacher

The headteacher will:

- Take responsibility for the day-to-day leadership and management of AI use in their school
- Liaise with the data protection officer (DPO) to ensure that the use of AI is in accordance with data protection legislation
- Ensure that the guidance set out in this policy is followed by all staff
- Ensure staff are appropriately trained in the effective use and potential risks of AI
- Make sure pupils are taught about the effective use and potential risks of AI
- Table requests for AI tool approval in KIT meetings with the director of data and technology
- Liaise with staff on their use of AI tools and ensure staff are at all possible times using only approved AI tools as defined in this policy and in particular appendix C1

C4.3 Data protection officer (DPO)

The data protection officer (DPO) is responsible for monitoring and advising on our compliance with data protection law, including in relation to the use of AI.

Our DPO is Dee Fullerton and is contactable via dpo@beckmeadtrust.org.

C4.4 Safeguarding lead

The safeguarding lead is responsible for monitoring and advising on our compliance with safeguarding requirements including in relation to the use of AI, such as:

- Being aware of new and emerging safeguarding threats posed by AI
- Updating and delivering staff training on AI safeguarding threats
- Responding to safeguarding incidents in line with Keeping Children Safe in Education (KCSIE)

C4.5 All staff

As part of our aim to reduce staff workload while improving outcomes for our pupils, we encourage staff to explore opportunities to meet these objectives through the use of approved AI tools. Any use of AI must follow the guidelines set out in this policy.

To protect data when using generative AI tools, staff must:

- Use approved AI tools (see section C5)
- Recognise that AI tools that are not approved are not supported or within any scope of support from the central IT services team and any staff member in the wider trust
- Seek advice from the data protection officer / central IT services / AI lead, as appropriate
- Check whether they are using an open or closed generative AI tool
- Ensure there is no identifiable information included in what they put into open generative AI tools
- Acknowledge or reference the use of generative AI in their work
- Fact-check results to make sure the information is accurate

All staff play a role in ensuring that pupils understand the potential benefits and risks of using AI in their learning. All of our staff have a responsibility to guide pupils in critically evaluating AI-generated information and understanding its limitations.

C4.6 Pupils

Pupils must:

- Follow the guidelines set out in section C7 of this policy ('Use of AI by pupils')

C5. Staff and governors use of AI

C5.1 Approved use of AI

We are committed to helping staff and governors reduce their workload. Generative AI tools can make certain written tasks quicker and easier to complete, but cannot replace the judgement and knowledge of a human expert.

Whatever tools or resources are used to produce plans, policies or documents, the quality and content of the final document remains the professional responsibility of the person who produced it.

Any plans, policies or documents created using AI should be clearly attributed. Any member of staff or governor using an AI-generated plan, policy or document should only share the AI-generated content with other members of staff or governors for use if they are confident of the accuracy of the information, as the content remains the professional responsibility of the person who produced it.

Always consider whether AI is the right tool to use. Just because the trust/school has approved its use doesn't mean it will always be appropriate.

Given how rapidly AI is evolving, please see the table in appendix C1 outlining current approved AI tools. Please note that this will be updated as and when we come across a new AI tool. Once an AI tool is approved for the trust/school the table in appendix C1 will be updated and published.

The approval process is outlined in section C5.2 of this policy.

C5.2 Process for approval

Staff are welcome to suggest new ways of using AI to improve pupil outcomes and reduce workload. Staff should contact the headteacher to discuss any ideas they may have with regards to using AI, so the headteacher can take the suggestions forward to the director of data and technology if they deem it to be a satisfactory new method of working. The headteacher will raise this in their KIT meetings with the director of data and technology to initiate the approval process.

The director of data and technology is responsible for signing off on approved uses of AI, or new AI tools, taking into account advice from the headteacher, the executive team at the trust, the DPO and data protection impact assessments.

C5.3 Data protection and privacy

To ensure that personal and sensitive data remains secure, no one will be permitted to enter such data into unauthorised generative AI tools or chatbots.

If personal and/or sensitive data is entered into an unauthorised generative AI tool, The Beckmead Trust will treat this as a data breach and will follow the personal data breach procedure outlined in our data protection policy (this policy can be found on the Beckmead Trust website). Please also see section C10 of this policy.

C5.4 Intellectual property

Most generative AI tools use inputs submitted by users to train and refine their models.

Pupils own the intellectual property (IP) rights to original content they create. This is likely to include anything that shows working out or is beyond multiple choice questions.

Pupils' work must not be used by staff to train generative AI models without appropriate consent or exemption to copyright.

Exemptions to copyright are limited – we will seek legal advice if we are unsure as to whether we are acting within the law.

C5.5 Bias

We are aware that AI tools can perpetuate existing biases, particularly towards special characteristics including sex, race and disability. This means that critical thought must be applied to all outputs of authorised AI applications. This means fact and sense-checking the output before relying on it.

We will ensure we can identify and rectify bias or error by training staff in this area.

We also regularly review our use of AI to identify and correct any biases that may arise.

If parents/carers or pupils have any concerns or complaints about potential unfair treatment or other negative outcomes due to AI use, these will be dealt with through our usual complaints procedure (this can be found on the Beckmead Trust website).

C5.6 Raising concerns

We encourage staff and governors to speak to the headteacher in the first instance if they have any concerns about a proposed use of AI, or the use of AI that may have resulted in errors that lead to adverse consequences or unfair treatment.

C5.7 Ethical and responsible use

We will always:

- Use generative AI tools ethically and responsibly
- Remember the principles set out in our trust/school's equality policy when using generative AI tools (this policy can be found on the Beckmead Trust website)
- Consider whether the tool has real-time internet access, or access to information up to a certain point in time, as this may impact the accuracy of the output
- Fact and sense-check the output before relying on it

Any Stakeholder (including but not limited to Pupils, Parents/Carers, Staff and Governors) must not:

- Generate content to impersonate, bully or harass another person
- Generate explicit or offensive content
- Input offensive, discriminatory or inappropriate content as a prompt

C5.8 Unwanted AI

Please see appendix C2 for guidance on how to deal with unwanted AI

C6. Educating pupils about AI

Here at The Beckmead Trust we acknowledge that pupils benefit from a knowledge-rich curriculum that allows them to become well-informed users of technology and understand its impact on society. Strong foundational knowledge will ensure that pupils develop the right skills to make the best use of generative AI.

Pupils are taught a curriculum that is personalised to their needs and equivalent key stage working level - the curriculum will endeavour to include the potential benefits of using AI tools to aid their learning, while also covering subjects such as:

- Creating and using digital content safely and responsibly
- The limitations, reliability and potential bias of generative AI
- How information on the internet is organised and ranked
- Online safety to protect against harmful or misleading content

C7. Use of AI by pupils

We recognise that AI has many uses to help pupils learn. Approved AI tools must be encouraged and used as the tool of choice unless there is a specific defined reason why it can not. This must be appropriately logged (either via a ticket with central IT services or with the headteacher).

*The below items contain examples but are not exhaustive lists - human judgement **must** be used in all cases where AI is used.*

Pupils may use AI tools:

- As a research tool to help them find out about new topics and ideas
- When specifically studying and discussing AI in trust/schoolwork, for example in IT lessons or art homework about AI-generated images
- To get differentiated content that is personalised to their particular needs

All AI-generated content must be properly attributed and appropriate for the pupils' age and educational needs.

AI may also lend itself to cheating and plagiarism. To mitigate this, pupils may not use AI tools:

- During assessments, including internal and external assessments, and coursework
- To write their homework or class assignments, where AI-generated text is presented as their own work
- To complete their homework, where AI is used to answer questions set and is presented as their own work (for example, maths calculations)

This list of AI misuse is not exhaustive.

Where AI tools have been used as a source of information, pupils should reference their use of AI. The reference must show the name of the AI source and the date the content was generated. It is important to note that we understand that there may be some scope where this requirement is supported by the staff team who work with the pupil.

We consider any unattributed use of AI-generated text or imagery to be plagiarism.

Pupils must consider what is ethical and appropriate in their use of AI and must not:

- Generate content to impersonate, bully or harass another person
- Generate explicit or offensive content
- Input offensive, discriminatory or inappropriate content as a prompt

C8. Formal assessments

We will continue to take reasonable steps where applicable to prevent malpractice involving the use of generative AI in assessments.

We will follow the latest guidance published by the Joint Council for Qualifications (JCQ) on AI use in assessments.

C9. Staff training

Staff will be kept up to date through a range of methods based on their position and responsibilities:

- Termly newsletters will share broad information about the impact, implementation and innovations in AI at Beckmead and within the wider world
- The Trust Landing Pages host a range of signposting, training, guidance and other relevant material for staff teams to reference and use in training
- Training packages will be available and shared via headteachers or line manager from the National College CPD platform
- The central IT services team will take part in an internal bespoke training programme that is developed in line with emerging technologies, risks and the team's skill sets on AI and other IT initiatives and systems - to ensure they are the 'experts'
- The DfE have provided a succinct video that all staff should watch to understand how to protect children's privacy when using AI: Protecting children's privacy when using Artificial Intellige…

C10. Breach of this policy

C10.1 By staff

Breach of this policy by staff will be dealt with in line with our staff code of conduct (this can be found on the Beckmead Trust website).

Where disciplinary action is appropriate, it may be taken whether the breach occurs:

- During or outside of working hours
- On an individual's own device or a trust/school device
- At home, at trust/school or from a remote working location

Staff members will be required to co-operate with any investigation into a suspected breach of this policy. This may involve providing us with access to:

- The generative AI application in question (whether or not it is one authorised by the trust/school)
- Any relevant passwords or login details

You must report any breach of this policy, either by you or by another member of staff, to the headteacher or a director immediately.

C10.2 By governors

Governors found in breach of this policy will be dealt with in line with our governor code of conduct (this can be found on the Beckmead Trust website).

C10.3 By pupils

Any breach of this policy by a pupil will be dealt with in line with our behaviour policy (this can be found on the Beckmead Trust website).

C11. Monitoring and transparency

AI technology, and the benefits, risks and harms related to it, evolves and changes rapidly. Consequently, this policy is a live document that must be kept updated by the director of data and technology whenever there is a significant change to either AI use by the trust/school or the associated risks of AI usage.

This policy will also be regularly reviewed and updated to align with emerging best practices, technological advancements and changes in regulations - at minimum annually.

The director of data and technology will monitor the effectiveness of AI usage across the trust/schools.

We will ensure we keep members of the trust/school community up to date on the use of AI technologies for educational purposes. As part of our regular surveys, feedback from pupils, parents/carers and staff will be considered in the ongoing evaluation and development of AI use in the trust/schools.

D) Mobile phone policy

D1. Introduction and aims

At the Beckmead Trust we recognise that mobile phones and similar devices, including smartphones, are an important part of everyday life for our pupils, parents/carers and staff, and the wider school community.

Our policy aims to:

- Promote safe and responsible phone use
- Set clear guidelines for the use of mobile phones for pupils, staff, parents/carers, visitors and volunteers
- Support the school's other policies, especially those related to child protection and behaviour

This policy also aims to address some of the challenges posed by mobile phones in school, such as:

- Risks to child protection
- Data protection issues
- Potential for lesson disruption
- Risk of theft, loss, or damage
- Appropriate use of technology in the classroom

Note: throughout this policy, 'mobile phones' refers to mobile phones and similar devices.

D2. Relevant guidance

This policy meets the requirements of the Department for Education's non-statutory mobile phone guidance and behaviour guidance. Further guidance that should be considered alongside this policy is Keeping Children Safe in Education.

D3. Roles and responsibilities

Details can be found in the Roles and responsibilities section of this policy

D4. Use of mobile phones by staff

The DfE's non-statutory mobile phone guidance says that staff should not use their own mobile phone for personal reasons in front of pupils throughout the school day.

Staff should not have their mobile phones out in classrooms or around pupils - e.g. not placed on tables when students are present.

The School/Trust accepts no liability for any devices damaged on school premises or on any school related activities and transportation.

D4.1 Personal mobile phones

Staff (including volunteers, contractors and anyone else otherwise engaged by the school) are not permitted to use their personal mobile phone, while children are present or during contact time. Use of personal mobile phones must be restricted to non-contact time, and to areas of the school where pupils are not present (such as the staffroom).

There may be circumstances in which it is appropriate for a member of staff to have use of their phone during contact time for personal reasons. For instance (this list is non-exhaustive):

- For emergency contact by their child, or their child's school
- In the case of acutely ill dependents or family members

The headteacher will decide on a case-by-basis whether to allow for special arrangements.

If special arrangements are not deemed necessary, school staff can use the school office number (which can be found on the Beckmead Trust website) as a point of emergency contact.

D4.2 Data protection

Staff must not use their personal mobile phones to process personal data, or any other confidential school information, including entering such data into generative artificial intelligence (AI) tools such as chatbots (e.g. ChatGPT and Google Gemini).

D4.3 Safeguarding

Staff must not give their personal contact details to parents/carers or pupils, including connecting through social media and messaging apps.

Staff must avoid publicising their contact details on any social media platform or website, to avoid unwanted contact by parents/carers or pupils.

Staff must not use their personal mobile phones to take photographs or recordings of pupils, their work, or anything else that could identify a pupil. If it's necessary to take photos or recordings as part of a lesson/school trip/activity, this must be done using school equipment.

D4.4 Using personal mobiles for work purposes

In some circumstances, it may be appropriate for staff to use personal mobile phones for work. Such circumstances may include, but are not limited to:

- Issuing homework, rewards or sanctions
- Use of multi-factor authentication
- Emergency evacuations
- Supervising off-site trips
- Supervising residential visits

In these circumstances, staff will:

- Use their mobile phones in an appropriate and professional manner, in line with our staff code of conduct
- Not use their phones to take photographs or recordings of pupils, their work, or anything else that could identify a pupil
- Refrain from using their phones to contact parents/carers. If necessary, contact must be made via the school office

D4.5 Work phones

The school provides some staff with a mobile phone for work purposes.

Only authorised staff are permitted to use school phones. Access to the phone must not be provided to anyone without authorisation.

Staff must:

- Only use phone functions for work purposes, including making/receiving calls, sending/receiving emails or other communications, or using the internet
- Ensure that communication or conduct linked to the device is appropriate and professional at all times, in line with our staff code of conduct

D4.6 Sanctions

Staff who do not follow this policy may face disciplinary action.

D5. Use of mobile phones by pupils

Each school will have particular arrangements for mobile devices that may override the below general practice model - if you require information on your school's exact arrangements please contact the headteacher or school office (email can be found on the Beckmead Trust website) for more information.

General practice model for Mobile Devices

Pupils may bring mobile devices into trust/school, but are not permitted to use them during:

- Lessons
- Tutor group time
- Clubs before or after trust/school, or any other activities organised by the trust/school

Mobile devices will be handed in to the teacher, office team or senior leaders at the beginning of the day and returned at the end of the day. Mobile devices will be securely stored.

Any use of mobile devices in trust/school by pupils must be in line with the acceptable use agreement (see appendices A3 and A4).

Any breach of the acceptable use agreement by a pupil may trigger disciplinary action in line with the trust/school behaviour policy, which may result in the confiscation of their device.

Residential settings will have specific arrangements and these will be outlined on the Beckmead Trust website under the provisions relevant policy.

D5.1 Use of smartwatches by pupils

The DfE's non-statutory mobile phone guidance includes in the term 'mobile phones' all devices with communications and smart technology that the school chooses to include in their policy.

Smartwatches are wristwatches with smart technology in them. They can be used to tell the time, send and receive text and voice messages, make calls and listen to music. Some smart watches have wellness and health-related features.

As above the general practice for mobile devices will be enforced unless the school has particular arrangements that override this.

D5.2 Exceptions

Exceptional circumstances will be considered on a case-by-case basis. To request such permission, pupils or parents/carers should contact the headteacher at the school.

Any pupils who are given permission must then adhere to all the guidance as outlined in this policy for mobile phone use (see appendix D1).

D5.3 Sanctions

Each school will have particular arrangements for mobile devices that may override the below general practice model - if you require information on your schools exact arrangements please contact the headteacher or school office (email can be found on the Beckmead Trust website) for more information.

The general practice model for sanctions related to Mobile Devices follows the DfE's guidance on mobile phones in schools

In each case, the sanction given must be reasonable and proportionate. The school will also consider whether:

- There are any relevant special circumstances (for example, age, religious requirements, special educational needs, disability)
- The pupil's behaviour may indicate they may be suffering, or at risk of, harm. If this is suspected, staff will follow the appropriate procedure set out in Part 1 of Keeping Children Safe in Education

Certain types of conduct, bullying or harassment can be classified as criminal conduct. The school takes such conduct extremely seriously and will involve the police or other agencies as appropriate.

Such conduct includes, but is not limited to:

- Sexting (consensual and non-consensual sharing nude or semi-nude images or videos)
- Upskirting
- Threats of violence or assault
- Abusive calls, emails, social media posts or texts directed at someone on the basis of someone's ethnicity, religious beliefs or sexual orientation

D6. Use of mobile phones by parents/carers, volunteers and visitors

Parents/carers, visitors and volunteers (including governors and contractors) must adhere to this policy as it relates to staff if they are on the school site during the school day.

This means:

- Not taking pictures or recordings of pupils, unless it's at a public event (such as a school fair), or of their own child
- Using any photographs or recordings for personal use only, and not posting on social media without consent
- Not using phones in lessons, or when working with pupils

Parents/carers, visitors and volunteers will be informed of the rules for mobile phone use when they sign in at reception or attend a public event at school.

The school office team will usually provide a summary of the rules prior to or upon arrival at the school.

Parents/carers or volunteers supervising school trips or residential visits must not:

- Use their phone to make contact with other parents/carers
- Take photos or recordings of pupils, their work, or anything else that could identify a pupil

Parents/carers or volunteers supervising trips are also responsible for enforcing the school's policy for pupils using their phones, as set out in section D5 above, but must refer any sanctions to a member of staff, as they do not have the power to search or confiscate devices.

Parents/carers must use the school office as the first point of contact if they need to get in touch with their child during the school day. They must not try to contact their child on their personal mobile during the school day.

D7. Loss, theft or damage

Pupils bringing mobile phones to school must ensure that the phones are appropriately labelled and are handed in to be stored securely as outlined in section D5.

Pupils must secure their mobile phones as much as possible, including using passwords or pin codes to protect access to the phone's functions. Staff must also secure their personal phones, and any work phone provided to them. Failure by staff to do so could result in data breaches.

Although the trust/school endeavours to keep personal devices safe, we cannot accept responsibility for mobile phones or any other personal devices that are lost, damaged or stolen on school premises or transport, during school visits or trips, or while pupils are travelling to and from school.

This disclaimer is in appendix A3 and A4 and should be signed off yearly by pupils and parents/carers.

Confiscated phones will be stored in the headteacher/senior leader or school office in a secure location / locked cabinet.

Lost phones should be returned to the school office. The school will try to contact the owner.

D8. Monitoring and review

The school is committed to ensuring that this policy has a positive impact on pupils' education, behaviour and welfare. When reviewing the policy, the school will take into account:

- Feedback from parents/carers and pupils
- Feedback from staff
- Records of behaviour and safeguarding incidents
- Relevant advice from the Department for Education, the local authority and any other relevant organisations

If there are any concerns regarding this policy, these should be brought to the attention of the headteacher in a timely manner.

E) ICT Disaster Recovery plan

E1. Introduction and aims

This section outlines the ICT Disaster Recovery Plan for The Beckmead Trust (TBT), ensuring the continuity and restoration of key ICT services in the event of an emergency.

E2. Key ICT Services

The Beckmead Trust relies on several mission-critical systems to fulfill its legal and statutory duties. These include:

- Data Email systems for timely information sharing and storage of data
- Management Information Systems (MIS) for logging and sharing pupil data
- Entry Management Systems for site access control
- Financial Systems for storing and processing financial data

These systems are operated according to the recommendations from suppliers, current IT protocols and government/statutory guidance. They are managed by the central IT services team directly or via a third-party support organization.

All systems are managed in accordance with the wider Digital Policy and the specific details outlined with this ICT Disaster Recovery Plan.

E4. Ensuring Continuity

The Beckmead Trust has the majority of its systems within or as Cloud Services. This minimizes the reliance on physical site infrastructure for critical services and enables some major parts of the organisation to operate from any location with internet connectivity. It also means that in the event of a site evacuation, The Beckmead Trust staff and pupils can continue to access their resources remotely.

E5. Restoration of Services in an Emergency

This ICT Disaster Recovery Plan details the mitigations in place to prevent the loss of critical services and establishes Service Levels that third-party suppliers must adhere to. The adoption of Cloud Services significantly reduces risks by eliminating dependence on on-site hosting of critical systems.

See E7 for more information.

E6. Ongoing Checks and Disaster Recovery Timeframes

This ICT Disaster Recovery Plan defines the timeframes within which any critical service must be restored. The plan is reviewed at least annually. The Beckmead Trust requires proof of restoration times from third-party companies to ensure they can meet The Beckmead Trust's needs.

E7. Mitigation Plans and Service Level Expectations

Category	Mitigation	Service Level Expectations
ICT Disasters Physical destruction of devices and equipment	Adoption of Cloud Services significantly reduces risks by eliminating dependence on on-site hosting of critical systems. Daily (and higher frequency automatic) backups of critical data to cloud-based systems not connected to the school network. Arbor data back-up off site so restore can take place.	Incident response plan tested every 6 months using the NCSC's 'Exercise in a Box'.
Cyber Security Supply Chain	Check that its supply chain is secure, for example by asking suppliers about how secure their business practices are and checking if they have the Cyber Essentials certification.	Expectation of suppliers adhering to security standards (e.g., Cyber Essentials).
Management Information System (MIS)	Delegate specific responsibility for maintaining the security of our MIS to our cloud-based provider with oversight from central IT services.	Cloud-based provider is expected to maintain MIS security; Oversight by central IT services for monitoring and accountability.
IT Software Security	Investigate whether our IT software needs updating or replacing to be more secure. Third party audits (such as Cyber Essentials or 360 degree safe) annually to objectively test that what it has in place is effective.	Controls in place will be: -Proportionate: verified via third-party audit. -Multi-layered. -Up to date: system in place to monitor software updates. -Regularly reviewed and tested.
Access to ICT	Cloud-based hosting of critical systems, daily backups, and incident response plan.	99.99% cloud services availibility
Phone Communications Loss	Phone systems (handsets and session border controller) can connect to 4G or 5G connection to enable a small number of key handsets to function onsite. School/Trust phone numbers can be diverted to handsets with VoIP app installed (or if necessary mobile phone numbers) to handle calls	Phone and critical communication systems restored within 4 hours (target). Initial acknowledgment of the incident from providers within 15 minutes. Regular updates (every hour or more frequently if critical) provided to key stakeholders
Internet Loss for significant periods of time	4G or 5G router to be obtained from current broadband provider, Mobile Phone supplier or other suitable entity and used to provide data connection. Evac ipad in central office is on separate 4G/5G connection for use in the event of internet downtime.	99.99% internet services uptime

Appendices

Appendix A1: Facebook cheat sheet for staff

Do not accept friend requests from pupils on social media

10 rules for trust/school staff on Facebook

1. Change your display name – use your first and middle name, use a maiden name, or put your surname backwards instead
2. Change your profile picture to something unidentifiable, or if you don't, make sure that the image is professional
3. Check your privacy settings regularly
4. Be careful about tagging other staff members in images or posts
5. Don't share anything publicly that you wouldn't be happy showing your pupils
6. Don't use social media sites during trust/school hours
7. Don't make comments about your job, your colleagues, our trust/school or your pupils online – once it's out there, it's out there
8. Don't associate yourself with the trust/school on your profile (e.g. by setting it as your workplace, or by 'checking in' at a trust/school event)
9. Don't link your work email address to your social media accounts. Anyone who has this address (or your personal email address/mobile number) is able to find you using this information
10. Consider uninstalling the Facebook app from your phone. The app recognises WiFi connections and makes friend suggestions based on who else uses the same WiFi connection (such as parents or pupils)

Check your privacy settings

- Change the visibility of your posts and photos to **'Friends only'**, rather than 'Friends of friends'. Otherwise, pupils and their families may still be able to read your posts, see things you've shared and look at your pictures if they're friends with anybody on your contacts list
- Don't forget to check your **old posts and photos** – go to bit.ly/2MdQXMN to find out how to limit the visibility of previous posts
- The public may still be able to see posts you've **'liked'**, even if your profile settings are private, because this depends on the privacy settings of the original poster
- **Google your name** to see what information about you is visible to the public
- Prevent search engines from indexing your profile so that people can't **search for you by name** – go to bit.ly/2zMdVht to find out how to do this
- Remember that **some information is always public**: your display name, profile picture, cover photo, user ID (in the URL for your profile), country, age range and gender

What to do if …

A pupil adds you on social media

- In the first instance, ignore and delete the request. Block the pupil from viewing your profile
- Check your privacy settings again, and consider changing your display name or profile picture
- If the pupil asks you about the friend request in person, tell them that you're not allowed to accept friend requests from pupils and that if they persist, you'll have to notify senior leadership and/or their parents/carers. If the pupil persists, take a screenshot of their request and any accompanying messages
- Notify the senior leadership team or the headteacher about what's happening

A parent/carer adds you on social media

- It is at your discretion whether to respond. Bear in mind that:
    - Responding to 1 parent/carer's friend request or message might set an unwelcome precedent for both you and other teachers at the trust/school
    - Pupils may then have indirect access through their parent/carer's account to anything you post, share, comment on or are tagged in
- If you wish to decline the offer or ignore the message, consider drafting a stock response to let the parent/carer know that you're doing so

You're being harassed on social media, or somebody is spreading something offensive about you

- **Do not** retaliate or respond in any way
- Save evidence of any abuse by taking screenshots and recording the time and date it occurred
- Report the material to Facebook or the relevant social network and ask them to remove it
- If the perpetrator is a current pupil or staff member, our mediation and disciplinary procedures are usually sufficient to deal with online incidents
- If the perpetrator is a parent/carer or other external adult, a senior member of staff should invite them to a meeting to address any reasonable concerns or complaints and/or request they remove the offending comments or material
- If the comments are racist, sexist, of a sexual nature or constitute a hate crime, you or a senior leader should consider contacting the police

Appendix A2: Acceptable use of the internet: agreement for parents and carers

Acceptable use of the internet: agreement for parents and carers	
Name of parent/carer: **Name of child:**	
Online channels are an important way for parents/carers to communicate with, or about, our trust/school. The trust/school uses the following channels: • Emails to the school office inbox or the central trust inbox • Arbor Parent Portal and SMS • Google Classroom • Each school may also have an official channel that they use - please confirm this with the school by contacting their office inbox (this can be found on the Beckmead Trust website) We also recognise that independent channels may be set up that are not part of the trust/school - but these are not organised or supported by the trust/schools.	
When communicating with the trust/school via official communication channels, or using private/independent channels to talk about the trust/school, I will: • Be respectful towards members of staff, and the trust/school, at all times • Be respectful of other parents/carers and children • Direct any complaints or concerns through the trust/school's official channels, so they can be dealt with in line with the trust/school's complaints procedure I will not: • Use private groups, the trust/school's Facebook page, or personal social media to complain about or criticise members of staff. This is not constructive and the trust/school can't improve or address issues unless they are raised in an appropriate way • Use private groups, the trust/school's Facebook page, or personal social media to complain about, or try to resolve, a behaviour issue involving other pupils. I will contact the trust/school and speak to the appropriate member of staff if I'm aware of a specific behaviour issue or incident • Upload or share photos or videos on social media of any child other than my own, unless I have the permission of the other children's parents/carers	
Signed:	**Date:**

Appendix A3: Acceptable use agreement for older pupils

Acceptable use of the trust/school's ICT facilities and internet: agreement for pupils and parents/carers

Name of pupil:

When using the trust/school's ICT facilities and accessing the internet in trust/school, I will not:

- Use them for a non-educational purpose
- Use them without a teacher being present, or without a teacher's permission
- Use them to break trust/school rules
- Access any inappropriate websites or use chat rooms
- Access social networking sites (unless my teacher has expressly allowed this as part of a learning activity)
- Open any attachments in emails, or follow any links in emails, without first checking with a teacher
- Use any inappropriate language when communicating online, including in emails
- Share any semi-nude or nude images, videos or livestreams, even if I have the consent of the person or people in the photo/video
- Share my password with others or log in to the trust/school's network using someone else's details
- Bully other people
- Log in to the trust/school's network using someone else's details
- Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision
- Use AI tools and generative chatbots (such as ChatGPT or Google Gemini):
    - During assessments, including internal and external assessments, and coursework
    - To present AI-generated text or imagery as my own work
    - To generate and create content, responses or information for which it is not made clear that AI was used

When I use the trust/school's ICT systems (like computers) and get onto the internet in trust/school I will:

- Keep my private information safe at all times and not give my name, address or telephone number to anyone without the permission of my teacher or parent/carer
- Tell a teacher (or sensible adult) immediately if I find any material that might upset, distress or harm me or others
- Always log off or shut down a computer when I've finished working on it

If I bring a personal mobile phone or other personal electronic device into trust/school:

- I will not use it during lessons, tutor group time, clubs or other activities organised by the trust/school, without a teacher's permission
- I will use it responsibly, and will not access any inappropriate websites or other inappropriate material or use inappropriate language when communicating online
- I understand that the trust/school accepts no responsibility for mobile devices that are lost, damaged or stolen on school premises or transport, during school visits or trips, or while pupils are travelling to and from school.

I understand that the trust/school will monitor the websites I visit and my use of the trust/school's ICT facilities and systems.

I will immediately let a teacher or other member of staff know if I find any material which might upset, distress or harm me or others.

I will always use the trust/school's ICT systems and internet responsibly.

I understand that the trust/school can discipline me if I do certain unacceptable things online, even if I'm not in trust/school when I do them.

Signed (pupil):	**Date:**

Parent/carer agreement: I agree that my child can use the trust/school's ICT systems and internet when appropriately supervised by a member of trust/school staff. I agree to the conditions set out above for pupils using the trust/school's ICT systems and internet, and for using personal electronic devices in trust/school, and will make sure my child understands these.

Signed (parent/carer):	**Date:**

Appendix A4: Acceptable use agreement for younger pupils

Acceptable use of the trust/school's ICT facilities and internet: agreement for pupils and parents/carers

Name of pupil:

When I use the trust/school's ICT systems (like computers) and get onto the internet in trust/school I will:

- Ask a teacher or adult if I can do so before using them and use them only when there is a teacher in the room
- Only use websites that a teacher or adult has told me or allowed me to use
- Always follow the trust/school rules
- Tell my teacher immediately if:
  - I select a website by mistake
  - I receive messages from people I don't know
  - I find anything that may upset or harm me or my friends
- Use trust/school computers for trust/school work only
- Be kind to others and not upset or be rude to them
- Look after the trust/school ICT equipment and tell a teacher straight away if something is broken or not working properly
- Only use the username and password I have been given
- Never share my password with anyone, including my friends
- Never give my personal information (my name, address or telephone numbers) to anyone without the permission of my teacher or parent/carer
- Save my work on the trust/school network
- Check with my teacher before I print anything
- Log off or shut down a computer when I have finished using it

When I use the trust/school's ICT facilities (like computers) and go on the internet in trust/school, I will not:

- Go on chat rooms, Facebook or other social networking sites (unless my teacher said I could as part of a lesson)
- Open any attachments in emails, or click any links in emails, without checking with a teacher first
- Use mean or rude language when talking to other people online or in emails
- Send any photos, videos or livestreams of people (including me) who aren't wearing all of their clothes
- Bully other people
- Use artificial intelligence (AI) chatbots, such as ChatGPT or Google Gemini, to create images or write for me, and then submit it as my own work

I understand that the trust/school will check the websites I visit and how I use the trust/school's computers and equipment. This is so they can help keep me safe and make sure I'm following the rules.

I will tell a teacher or a member of staff I know immediately if I find anything on a trust/school computer or online that upsets me, or that I know is mean or wrong.

I will always be responsible when I use the trust/school's ICT systems and internet.

I understand that the trust/school accepts no responsibility for mobile devices that are lost, damaged or stolen on school premises or transport, during school visits or trips, or while pupils are travelling to and from school.

I agree to the trust/school monitoring activity/websites I visit & that there will be consequences if I don't follow the rules.

Signed (pupil):	**Date:**

Parent/carer agreement: I agree that my child can use the trust/school's ICT systems and internet when appropriately supervised by a member of trust/school staff. I agree to the conditions set out above for pupils using the trust/school's ICT systems and internet, and for using personal electronic devices in trust/school, and will make sure my child understands these.

Signed (parent/carer):	**Date:**

Appendix A5: Acceptable use agreement for staff, governors, volunteers and visitors

Acceptable use of the trust/school's ICT facilities and the internet: agreement for staff, governors, volunteers and visitors

Name of staff member/governor/volunteer/visitor:

When using the trust/school's ICT facilities and accessing the internet in trust/school, or outside trust/school on a work device, I will not:

- Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material)
- Use them in any way which could harm the trust/school's reputation
- Access social networking sites or chat rooms
- Use any improper language when communicating online, including in emails or other messaging services
- Install any unauthorised software, or connect unauthorised hardware or devices to the trust/school's network
- Share my password with others or log in to the trust/school's network using someone else's details
- Take photographs of pupils without checking with teachers first
- Share confidential information about the trust/school, its pupils or staff, or other members of the community
- Access, modify or share data I'm not authorised to access, modify or share
- Promote any private business, unless that business is directly related to the trust/school

I understand that:

- Staff using work devices outside the Trust must ensure their security.
- Personal use of Trust phones is restricted.
- The use of AI tools is permitted for business purposes subject to specific conditions, including data privacy, output ownership, accuracy verification, and transparency
- Personal or confidential information must not be entered into unauthorized/unapproved AI tools or any other digital platform
- Unauthorized use of AI, especially during assessments or to plagiarize work, is prohibited
- Breaches of this agreement may result in disciplinary action or revocation of access privileges
- By using The Beckmead Trust's ICT facilities and internet access, you acknowledge that you have read, understood, and agree to abide by this Acceptable Use Agreement
- The Trust reserves the right to monitor the use of its ICT facilities and network, including internet sites visited, email accounts, and user activity, for safeguarding, security, and policy compliance purposes

I agree and understand that the trust/school will monitor the activity & websites I visit and my use of the trust/school's ICT facilities and systems.

I will only use the trust/school's ICT systems and access the internet in trust/school, or outside trust/school on a work device, for educational purposes or for the purpose of fulfilling the duties of my role.

I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside trust/school, and keep all data securely stored in accordance with this policy and the trust/school's data protection policy.

I will let the designated safeguarding lead (DSL) and Central IT Services know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material.

I will always use the trust/school's ICT systems and internet responsibly, and ensure that pupils in my care do so too.

I will use AI tools in line with the latest policy and follow the appropriate safeguards and protocols to ensure any AI tool use I undertake is appropriate and responsible.

I understand that the trust/school accepts no responsibility for personal devices that are lost, damaged or stolen on school premises or transport, during school visits or trips, or while staff are travelling between or to and from sites.

Signed (staff member/governor/volunteer/visitor):	**Date:**

Appendix A6: Glossary of cyber security terminology

These key terms will help you to understand the common forms of cyber attack and the measures the trust/school will put in place. They're from the National Cyber Security Centre (NCSC) glossary.

TERM	DEFINITION
Antivirus	Software designed to detect, stop and remove malicious software and viruses.
Breach	When your data, systems or networks are accessed or changed in a non-authorised way.
Cloud	Where you can store and access your resources (including data and software) via the internet, instead of locally on physical devices.
Cyber attack	An attempt to access, damage or disrupt your computer systems, networks or devices maliciously.
Cyber incident	Where the security of your system or service has been breached.
Cyber security	The protection of your devices, services and networks (and the information they contain) from theft or damage.
Download attack	Where malicious software or a virus is downloaded unintentionally onto a device without the user's knowledge or consent.
Firewall	Hardware or software that uses a defined rule set to constrain network traffic – this is to prevent unauthorised access to or from a network.
Hacker	Someone with some computer skills who uses them to break into computers, systems and networks.
Malware	Malicious software. This includes viruses, trojans or any code or content that can adversely impact individuals or organisations.
Patching	Updating firmware or software to improve security and/or enhance functionality.

TERM	DEFINITION
Pentest	Short for penetration test. This is an authorised test of a computer network or system to look for security weaknesses.
Pharming	An attack on your computer network that means users are redirected to a wrong or illegitimate website even if they type in the right website address.
Phishing	Untargeted, mass emails sent to many people asking for sensitive information (such as bank details) or encouraging them to visit a fake website.
Ransomware	Malicious software that stops you from using your data or systems until you make a payment.
Social engineering	Manipulating people into giving information or performing specific actions that an attacker can use.
Spear-phishing	A more targeted form of phishing where an email is designed to look like it's from a person the recipient knows and/or trusts.
Trojan	A type of malware/virus designed to look like legitimate software that can be used to hack a victim's computer.
Two-factor/multi-factor authentication	Using 2 or more different components to verify a user's identity.
Virus	Programmes designed to self-replicate and infect legitimate software programs or systems.
Virtual private network (VPN)	An encrypted network allowing remote users to connect securely.
Whaling	Highly- targeted phishing attacks (where emails are made to look legitimate) aimed at senior people in an organisation.

Appendix B1: Annual risk assessment template - considering and reflecting on the risks pupils face online

Risk Category	Specific Risk	Potential Impact on Pupils	Current Safeguards/ Controls	Further Actions/ Recommendations	Date Completed/ Reviewed
Content	Exposure to inappropriate content (e.g., pornography, hate speech, violence)	Emotional distress, anxiety, desensitization, distorted views of the world	Filtering through Firewall & OS platform tools Monitoring through Senso Staff supervision	Further refinement of filtering and monitoring tools Training for staff to be reviewed at school level	March 2025
Contact	Online grooming or exploitation by adults	Physical and emotional harm, trauma, abuse	Monitoring through Senso Staff supervision, relationships and insight/ observations	Further refinement of filtering and monitoring tools Training for staff to be reviewed at school level	March 2025
Conduct	Cyberbullying or harassment of other pupils	Emotional distress, isolation, anxiety, depression	Monitoring through Senso Staff supervision, relationships and insight/ observations	Further refinement of filtering and monitoring tools Training for staff to be reviewed at school level	March 2025
Commerce	Online scams, phishing, or financial exploitation	Financial loss, identity theft, data breaches	Staff training Penetration tests Active surveying to identify vulnerable staff	Cyber Essentials Plus certification to be finalised Vulnerable staff identification for training	March 2025
Data Privacy	Sharing personal information online with strangers or on unsecured platforms Open AI tool models	Identity theft, privacy violations, potential for misuse of information	Teaching and Learning for Students and Training for Staff Zero Trust network Access to closed AI tool	Data stops with reminders and warnings Limiting and blocking unapproved AI tools	March 2025
AI Risks	Misuse of AI tools for bullying or creating deepfakes Plagiarism or using AI to create content as own work or responses	Emotional distress, reputational damage, potential for manipulation	Teaching and Learning for Students and Training for Staff Monitoring through Senso Staff supervision, relationships and insight/ observations Access to closed AI tool	Training for staff to be reviewed at school level Limiting and blocking unapproved AI tools	March 2025

Appendix B2: Digital Safety Resources

For Students:

- Common Sense Media:
    - Link: https://www.commonsense.org/education/digital-citizenship
    - Details: Offers a comprehensive K-12 Digital Citizenship Curriculum covering topics like media balance, cyberbullying, online privacy, and news and media literacy. Includes lesson plans, videos, and interactive activities.
    - Relevance: Wide range of age-appropriate materials, well-structured, and widely respected.
- Thinkuknow (National Crime Agency - CEOP):
    - Link: https://www.thinkuknow.co.uk/
    - Details: Provides age-appropriate resources for children and young people aged 4-18, covering online safety topics like online grooming, social networking, and gaming. Includes interactive games, videos, and advice.
    - Relevance: UK based, and created by the National Crime Agency, very reliable information.
- Internet Matters:
    - Link: https://www.internetmatters.org/
    - Details: Offers practical advice and resources for parents and children on a range of online safety issues, including cyberbullying, online gaming, and social media. Provides age-specific guides and expert advice.
    - Relevance: Great for a wide range of topics, and easy to understand guides.
- Google's Be Internet Awesome:
    - Link: https://beinternetawesome.withgoogle.com/en_us
    - Details: Interactive game-based curriculum that teaches kids the fundamentals of digital citizenship and safety. Covers topics like sharing with care, not falling for fake, securing your secrets, it's cool to be kind, and when in doubt, talk it out.
    - Relevance: Engaging and fun for younger students, developed by a major tech company.

For Staff:

- SWGfL (South West Grid for Learning):
    - Link: https://swgfl.org.uk/
    - Details: Offers a range of online safety training and resources for schools, including online safety audits, training courses, and policy templates. Provides expert advice and support on all aspects of online safety.
    - Relevance: UK based, and provides resources that are very helpful for schools.
- UK Safer Internet Centre:
    - Link: https://saferinternet.org.uk/
    - Details: Provides resources and advice for schools on a range of online safety issues, including cyberbullying, online grooming, and social media. Offers training courses, webinars, and online safety tools.
    - Relevance: A national resource, providing up to date information.
- NSPCC (National Society for the Prevention of Cruelty to Children):
    - Link: https://learning.nspcc.org.uk/training

- Details: Offers training courses and resources for professionals working with children, including online safety training. Covers topics like online sexual abuse, cyberbullying, and sexting.
- Relevance: Focuses on safeguarding, a critical aspect of online safety.

- Google - Get started with Google AI in education
  - Link: https://goo.gle/aiskills-foredu
  - Details: Discover Google's courses and materials designed to help today's educators, students and their families thrive in an AI-driven world.
  - Relevance: Helping equip students, parents, educators and schools with the skills and tools to use AI responsibly and effectively

For Parents/Guardians:

- Internet Matters:
  - Link: https://www.internetmatters.org/
  - Details: (As mentioned above) Provides age-specific guides, expert advice, and resources for parents on a range of online safety issues.
  - Relevance: Very good parent focused resources.
- Parent Zone:
  - Link: https://parentzone.org.uk/
  - Details: Offers expert advice and resources for parents on a range of online safety issues, including social media, gaming, and online bullying. Provides practical tips and guidance to help parents keep their children safe online.
  - Relevance: Designed to help parents navigate the digital world.
- Connect Safely:
  - Link: https://www.connectsafely.org/
  - Details: Provides research-based safety tips, parents' guide, and resources on social media, mobile, and other online safety topics.
  - Relevance: Provides well researched information.
- Google Guardian's Guide to AI in Google for Education and Family Guide to AI
  - Links:
    - Guardian's Guide to AI in Google for Education
      https://services.google.com/fh/files/misc/guardians_guide_to_ai_in_education.pdf
    - Family Guide to AI

      https://services.google.com/fh/files/misc/family-guide-to-ai.pdf
  - Details: Google developed a Guardian's Guide to AI along with a conversation guide to support families in exploring AI together.
  - Relevance: These build on programs such as Be Internet Awesome and Online Safety Roadshows, which have helped millions of kids learn how to safely and confidently explore the online world.

Appendix B3: Posters

LGFL Six Top Tips

LGfL SafeguardED

SIX TOP TIPS

For Parents To Keep Your Children Safe Online

Most parents & carers think their children and young people spend too much time on devices. DON'T FEEL BAD! Lots of it is perfectly healthy anyway. Instead, follow these tips to keep them safe, happy and healthy.

Don't worry about screen time; aim for screen quality

Scrolling through social media isn't the same as making a film or story, or video calling Grandma. Use the Children's Commissioner's 'Digital Five A Day' to plan or review each day together.

Check the safety settings are turned on

Whether it's your home internet, mobile devices, consoles, apps or games, there are lots of settings to make them safer. The key ones are - can they chat to strangers, can they video chat or 'go live', are their posts public? What about safe search and Youtube? See parentsafe.lgfl.net for more.

Get your children to show you their apps and games

You don't need to know all about the latest app or game, but if your child shows you what they are doing and with whom, you'll probably see if it's appropriate or not. Remember 18 games are not more advanced – they are harmful to children! For parent guides to apps, including recommendations for kidsafe apps and video platforms, search for Common Sense Media reviews.

Don't try to hide news about scary things in the news

If you don't talk about it, your children might read inappropriate pages, believe scare stories or simply catastrophise in their heads. Why not watch Newsround together and talk about how they feel – there is guidance from Childline to help you.

Remind them of key online safety principles

There are too many to list, but remember human behaviour is the same online and offline. Remind your children to be a good friend, to ask for help if they are worried or if someone is mean, not to get undressed on camera and most important of all… if somebody tells them not to tell or ask for help because it's too late or they will get in trouble, THAT'S A LIE!

If you aren't sure, ASK!

Your school may be able to give you advice, but there are plenty of other places to ask for help as a parent or a child, whether it is advice or help to fix something. Lots of sites are listed at reporting.lgfl.net, including ones to tell your kids about (they might not want to talk to you in the first instance).

Follow the links above, visit parentsafe.lgfl.net for much more or follow @LGfLSafeguardED on Twitter or Facebook

the beckmead trust

JCQ AI and Assessments - a quick guide for students

JCQ CIC

AI and Assessments
A quick guide for students

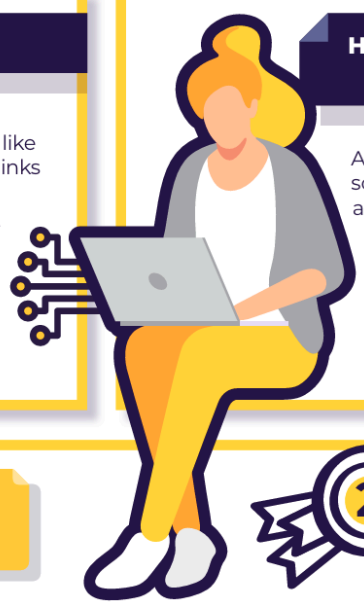
What is AI?

- AI stands for artificial intelligence and using it is like having a computer that thinks
- AI tools like ChatGPT or Snapchat My AI can write text, make art and create music by learning from data from the internet, but watch out – they can also make things up and be biased

How can AI be misused in assessments?

AI misuse is when you take something made using AI and say it's your own work.

THIS IS CHEATING!



How do I make sure I don't misuse AI?

1 Know the rules

- You're **not allowed** to use AI tools when you're in an exam
- Your teachers will tell you if you're allowed to use AI tools when doing your coursework – the rules will depend on your qualification
- Even if you're allowed to use AI tools, you can't get marks for content just produced by AI – your marks come from showing your own understanding and producing your own work

2 Reference reference reference! If you're allowed to use AI tools, you must reference them clearly

- Name the AI tool you used
- Add the date you generated the content
- Explain how you used it
- Save a screenshot of the questions you asked and the answers you got

3 Declare it's all your own work – When you hand in your assessment, you have to sign a declaration. Anything without a reference must be all your own work. If you've used an AI tool, don't sign the declaration until you're sure you've added all the references

What happens if I misuse AI?

If you've misused AI, you could lose your marks for the assessment – you could even be disqualified from the subject.

DON'T RISK IT!

REMEMBER

Misusing AI is cheating!

Know the rules

Talk to your teachers

Reference clearly

Preventing AI Misuse in Assessments - A summary for teachers

JCQ CIC Preventing AI Misuse in Assessments
A summary for teachers

As artificial intelligence (AI) technology is rapidly evolving, it's essential you understand how it can be used and misused within assessments. This summary provides key points to consider, to make sure assessment is fair for all.

1 Know your school or college's approach to managing AI in assessments

- Know what AI is and how it can be used
- Familiarise yourself with the JCQ *AI Use in Assessments* guidance
- Know what the risks are and how your school or college is managing them
- Understand how the approach applies to your subject

REMEMBER

Your malpractice policy MUST include the use of AI

- What AI is
- The risks of using AI
- What AI misuse is
- How AI misuse will be treated as malpractice
- When AI may be used
- How AI should be acknowledged

You're responsible for confirming the authenticity of students' work!

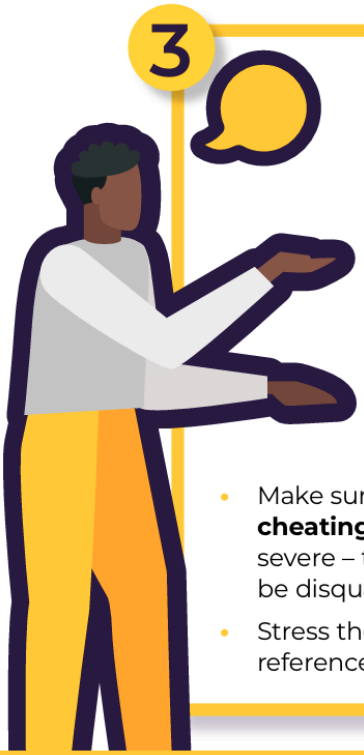
2 Plan how to prevent AI misuse in assessments

- If possible, find time for students to complete work under exam-like conditions/in class to help you understand the standard they are currently working at
- Talk to students about their work to check their understanding on an ongoing basis – before you start marking

the beckmead trust

JCQ CIC

Preventing AI Misuse in Assessments
A summary for teachers



3

Communicate the approach to students and parents/carers

- Be clear about when and if students can use AI tools
- If the qualification rules allow the use of AI tools, make sure students know how to reference clearly
- Remind students that any content produced using AI must be referenced and cannot be given marks – and a failure to reference use of AI is malpractice
- Make sure students and parents know that misusing AI is **cheating** and a form of malpractice. The consequences are severe – they could lose the marks for the assessment or even be disqualified from the subject
- Stress the importance of the candidate declaration (which references AI use) when they submit their work for assessment

If you suspect AI misuse...

4

Only accept work for assessment you consider to be the student's own!

- Compare with previous work for differences in quality, formatting, spelling, punctuation, grammar, vocabulary and tone
- Look out for AI indicators, for example, language style, lack of local knowledge, confidently wrong statements
- Consider the use of AI detection tools and discussing the work with the student as part of a holistic approach

IF YOU FIND AI MISUSE

If the student hasn't signed the declaration form, follow your school or college's malpractice policy

If the declaration form has already been signed, report to the awarding body

For more details, see the JCQ booklet –
AI Use in Assessments: Protecting the Integrity of Qualifications

Appendix B4: online safety training needs – self-audit for staff

ONLINE SAFETY TRAINING NEEDS AUDIT	
Name of staff member/volunteer:	**Date**:
Question	**Yes/No (add comments if necessary)**
Do you know the name of the person who has lead responsibility for online safety in trust/school?	
Are you aware of the ways pupils can abuse their peers online?	
Do you know what you must do if a pupil approaches you with a concern or issue?	
Are you familiar with the trust/school's acceptable use agreement for staff, volunteers, governors and visitors?	
Are you familiar with the trust/school's acceptable use agreement for pupils and parents/carers?	
Are you familiar with the filtering and monitoring systems on the trust/school's devices and networks?	
Do you understand your role and responsibilities regarding filtering and monitoring?	
Do you regularly change your password for accessing the trust/school's ICT systems?	
Are you familiar with the trust/school's approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/further training?	

Appendix B5: online safety incident report log

ONLINE SAFETY INCIDENT LOG				
Date	**Where the incident took place**	**Description of the incident**	**Action taken**	**Name and signature of staff member recording the incident**

Appendix C1: Approved AI Tools

Currently there are **4** tools that are approved in the table below:

Approved tools	Who is Approved to use it	Approved uses	Open or Closed AI
Google Gemini via a @beckmeadtrust.org email	Students Staff	<u>Content Generation and Brainstorming (with careful review):</u> • Generating initial drafts of documents, emails, or announcements. • Brainstorming ideas for lesson plans, projects, or activities. • Developing outlines or structures for written materials. • Creating varied text formats for internal communications (e.g., summaries, bullet points). • Generating creative content for staff engagement (e.g., icebreaker questions, team-building prompts). <u>Summarisation and Information Extraction:</u> • Summarising lengthy documents, articles, or research papers for quicker understanding. • Extracting key information and action items from meeting transcripts or notes. • Condensing information from various sources for internal reports or presentations. <u>Translation and Language Assistance:</u> • Translating text for communication with staff or stakeholders who speak different languages. • Improving the clarity and grammar of written materials. <u>Research and Information Gathering (critical evaluation required):</u> • Quickly gathering background information on a topic for professional development or curriculum research. • Identifying potential resources or examples to enhance teaching materials. • Exploring different perspectives on educational topics. (Crucially, emphasise the need for fact-checking and verifying information from Gemini with reliable sources.) <u>Administrative Task Assistance:</u> • Drafting templates for common administrative tasks (e.g., permission slips, feedback forms). • Generating ideas for improving internal processes or workflows. • Creating initial versions of training materials or guides for staff. <u>Accessibility and Inclusion Support:</u> • Generating alternative text descriptions for images to improve the accessibility of internal documents. • Simplifying complex language in communications for broader understanding. <u>Professional Development and Learning:</u> • Exploring new pedagogical approaches or educational technologies. • Summarising key takeaways from professional development articles or videos. • Generating questions for self-reflection on teaching practices. *Other appropriate uses in line with the Digital Policy*	Closed

KeyGPT via a @beckmeadtrust .org email	Staff	Some of the above plus: Letter to parents/carers Job descriptions and adverts Interview questions	Closed
Oak Academy AI lesson planner	Staff	Lesson planning	Open
Canva AI via a @beckmeadtrust .org email	Students Staff	Appropriate design uses including but not limited to above	*Closed

Open generative AI tools can be accessible and modifiable by anyone. They may store, share or learn from the information entered into them, including personal or sensitive information.

Closed generative AI tools are generally more secure, as external parties cannot access the data you input.

*__Do not adjust your settings when using Canva AI.__ https://www.canva.com/trust/privacy/: *"Canva does not train AI on your user content, unless you enable the setting in your Privacy Settings."*

Appendix C2: Unauthorised and Unwanted AI tools

Within the Beckmead Trust's context, an "Unauthorised and Unwanted AI tool" is defined as any artificial intelligence application, software, or service that meets one or more of the following criteria:

1. **Unauthorized Installation or Subscription:** The tool has been installed, downloaded, or subscribed to by a staff member (or any authorised user) without obtaining the required approval from authorised personnel, such as the Director of Data and Technology or Headteacher, as outlined in the Trust's Digital Policy (specifically sections C5 and C5.2).
2. **Data Security and Privacy Risks:** The tool poses a potential risk to the security, confidentiality, or integrity of the Trust's data, including personal data. This includes tools that may transmit data to external servers, store data insecurely, or violate data protection regulations (e.g., UK GDPR).
3. **Policy Non-Compliance:** The tool's use contradicts or violates specific provisions of the Trust's Digital Policy, such as guidelines on AI usage (section C), acceptable use (section A4), data security (section A8), or online safety (section B). This includes using tools for prohibited activities or in ways that are explicitly disallowed.
4. **Lack of Understanding or Awareness:** The staff member installing or subscribing to the tool may not fully understand its functionalities, data handling practices, or potential risks, leading to unintentional policy breaches or security vulnerabilities.
5. **Unsupported or Unmanaged:** The tool is not supported by the Trust's central IT services, meaning there is no official guidance, maintenance, or security oversight for its use. This can lead to compatibility issues, security vulnerabilities, or data loss.

In essence, an "unwanted AI tool" is any AI tool that is brought into the Trust's environment without proper authorization, poses risks to data or security, violates Trust policies, or is otherwise deemed inappropriate or unmanaged by the Trust's authorized personnel. It's important to note that the "unauthorised" or "unwanted" status of an AI tool isn't necessarily about the tool itself but how it is being used and whether it aligns with the Trust's established policies and procedures.

Examples of "unauthorised" or "unwanted" AI tools are listed below:

1. Otter AI
2. Read AI

Steps you can take if you have an "unauthorised" or "unwanted" AI attached to your account or device:

1. Remove from meetings manually by "kicking out" the AI before the meeting starts (it is important to be transparent about what is happening with the other participants of the meeting)
2. Login to "unauthorised" or "unwanted" AI tools portal and delete the account and all data created as a result of being involved with the AI tool
3. Contact central IT services for support if there is support needed to action any point related to this matter

<u>Furhter Notes on "unauthorised" or "unwanted" AI</u>

If you see an AI in a meeting (it appears as a invitee) - try to delete it

If it presents with you a link do not open it and DO NOT CLICK AGREE

If you can't delete it, please ask the meeting lead if they are aware of it and if they are, ask what it is for?

If you do not feel comfortable with it in the meeting, either request for it to be deleted or leave the meeting.

Many AI meeting notetakers act as a virus and once you accept it it will infiltrate your account and appear on your meetings. A particular drawback is the sharing of any minutes, without your consent or a chance to verify.

Appendix D1: Code of conduct/acceptable use agreement for pupils allowed to bring their phones to school due to <u>exceptional circumstances</u>

You must obey the following rules if you bring your mobile phone to school:

1. You may not use your mobile phone during lessons, unless the teacher specifically allows you to.
2. Phones must be switched off (not just put on 'silent').
3. You may not use your mobile phone in the toilets or changing rooms. This is to protect the privacy and welfare of other pupils.
4. You cannot take photos or recordings (either video or audio) of school staff or other pupils without their consent.
5. Avoid sharing your contact details with people you don't know, and don't share other people's contact details without their consent.
6. Don't share your phone's password(s) or access code(s) with anyone else.
7. Don't use your mobile phone to bully, intimidate or harass anyone. This includes bullying, harassing or intimidating pupils or staff via:
    a. Email
    b. Text/messaging app
    c. Social media
8. Don't use your phone to send or receive anything that may be criminal. For instance, by 'sexting'.
9. Rules on bullying, harassment and intimidation apply to how you use your mobile phone even when you aren't in school.
10. Don't use vulgar, obscene or derogatory language while on the phone or when using social media. This language is not permitted under the school's behaviour policy.
11. Don't use your phone to view or share pornography or other harmful content.
12. You must comply with a request by a member of staff to switch off, or hand over, a phone. Refusal to comply is a breach of the school's behaviour policy and will be dealt with accordingly.
13. Mobile phones are not permitted in any internal or external exam or test environment. If you have a mobile phone, you will be asked to store it appropriately, or turn it over to an exam invigilator, before entering the test room. Bringing a phone into the test room can result in your exam being declared invalid.

Appendix D2: Template mobile phone information slip for visitors

Print out and cut copies of this slip to give to visitors when they arrive at your school.

Use of mobile phones and similar devices in our school

- Please keep your mobile phone on silent/vibrate while on the school grounds
- Please do not use phones where pupils are present. If you must use your phone, you may go to _____
- Do not take photos or recordings of pupils (unless it is your own child), or staff
- Nothing should be shared online or via social media
- Do not use your phone in lessons, or when working with pupils

The school accepts no responsibility for phones that are lost, damaged or stolen while you are on the school grounds.

A full copy of our mobile phone policy is available from the school office.

Use of mobile phones and similar devices in our school

- Please keep your mobile phone on silent/vibrate while on the school grounds
- Please do not use phones where pupils are present. If you must use your phone, you may go to _____
- Do not take photos or recordings of pupils (unless it is your own child), or staff
- Nothing should be shared online or via social media
- Do not use your phone in lessons, or when working with pupils

The school accepts no responsibility for phones that are lost, damaged or stolen while you are on the school grounds.

A full copy of our mobile phone policy is available from the school office.

Use of mobile phones and similar devices in our school

- Please keep your mobile phone on silent/vibrate while on the school grounds
- Please do not use phones where pupils are present. If you must use your phone, you may go to _____
- Do not take photos or recordings of pupils (unless it is your own child), or staff
- Nothing should be shared online or via social media
- Do not use your phone in lessons, or when working with pupils

The school accepts no responsibility for phones that are lost, damaged or stolen while you are on the school grounds.

A full copy of our mobile phone policy is available from the school office.

Monitoring and review

The director of data and technology monitors the implementation of this policy, including ensuring it is updated to reflect the needs and circumstances of the trust/school.

This policy will be reviewed annually.

Related policies

This policy should be read alongside the trust/school's policies on:

- Safeguarding and child protection
- Behaviour
- Data protection
- Exams
- Staff code of conduct
- Equality
- Complaints procedure
- Business Continuity and Disaster Recovery