BECKFOOT TRUST

ONLINE SAFETY & IT USE POLICY

V7

November 2023

CREATING REMARKABLE SCHOOLS

Table of Contents

1.0 Policy Statement

1.1 Beckfoot Trust recognises that the use of technology has become a significant component of many safeguarding issues, including Child Sexual Exploitation, radicalisation, peer on peer abuse and sexual harassment, and understands that technology can be used as a platform to facilitate harm.

1.2 Beckfoot Trust aims to protect and educate students in their use of technology and has in place mechanisms to identify, intervene in, and escalate any incident where appropriate. It recognises the particular vulnerability of students with SEND online.

1.3 Beckfoot Trust ensures that each school has appropriate filters and monitoring systems in place to safeguard children from potentially harmful and inappropriate online material and does all it reasonably can to limit students' exposure to the above risks from the School's IT system Students' access to the internet via their personal mobile devices on school premises is limited and regulated.

2.0 Scope and Purpose

2.1 DFE Guidance

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

- Filtering and monitoring standards for schools and colleges
- Preventing and tackling bullying Advice for headteachers, staff and governing bodies
- Cyberbullying: Advice for headteachers and school staff
- Relationships and sex education (RSE) and health education
- Searching, screening and confiscation at school
- Protecting children from radicalisation
- Harmful online challenges and online hoaxes
- Sharing nudes and semi-nudes: advice for education settings working with children and young people

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

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

2.2 Links with other Trust policies:

- Trust Child Protection and Safeguarding Policy
- Trust Behaviour Policy
- Trust Disciplinary Policy and Grievance Procedure
- Trust GDPR, Data Protection and FOI Policy
- Trust Privacy Notices
- Trust Complaints Policy
- Trust Code of Conduct

3.0 Overarching Principles

3.1 Four 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, such as pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism

Contact – being subjected to harmful online interaction with other users, such as 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 – personal online behaviour that increases the likelihood of, or causes, harm, such as 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 scam

4.0 Responsibilities and Arrangements

4.1 The Trust Board and CEO

The Trust Board has overall responsibility for monitoring this policy and holding the CEO to account for its implementation.

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

The Board Member who oversees online safety is Paul Hill.

All Board members will:

- Ensure that they have read and understand this policy.
- Agree and adhere to the terms on acceptable use of the Trust IT systems and the internet (Appendix 2).
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with SEND 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.

4.2 Trust Executive Leaders with Responsibility for Safeguarding and IT

The DfE Filtering and monitoring standards for schools and colleges expects that senior leaders are responsible for:

- procuring filtering and monitoring systems
- documenting decisions on what is blocked or allowed and why
- reviewing the effectiveness of your provision
- overseeing reports

They are also responsible for making sure that all staff:

- understand their role

- are appropriately trained
- follow policies, processes and procedures
- act on reports and concerns

Executive leaders should work closely with trustees, the designated safeguarding leads and IT service providers in all aspects of filtering and monitoring. Your IT service provider may be a staff technician or an external service provider.

The IT service provider should work with the senior leadership team and DSL to:

- procure systems
- identify risk
- carry out reviews
- carry out checks

4.3 The Headteacher

The Headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

The school has undertaken the advised 360 evaluation of online safety (360 safe website) and has an action plan where any gaps have been identified

4.4 The Designated Safeguarding Lead

Details of the school Designated Safeguarding Lead (DSL) and Deputies are set out in the school protocol.

Day to day management of filtering and monitoring systems requires the specialist knowledge of both safeguarding and IT staff to be effective. The DSL should work closely together with IT service providers to meet the needs of the setting and may need to ask filtering or monitoring providers for system specific training and support.

The DfE Filtering and monitoring standards for schools and colleges expect that the DSL should take lead responsibility for safeguarding and online safety, which could include overseeing and acting on:

- filtering and monitoring reports
- safeguarding concerns
- checks to filtering and monitoring systems

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

- Supporting the Headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the Headteacher, IT Manager and other staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the school child protection policy
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety
- Liaising with other agencies and/or external services if necessary

- Providing regular reports on online safety in school to the headteacher and/or Trust Board

This list is not intended to be exhaustive.

4.5 IT Leadership

The DfE Filtering and monitoring standards for schools and colleges expect that the IT leadership should have technical responsibility for:

- maintaining filtering and monitoring systems
- providing filtering and monitoring reports
- completing actions following concerns or checks to systems

The Service Development Leader is responsible for:

- Putting in place an appropriate level of security protection procedures in line with the DFE Filtering and monitoring standards for schools and colleges.
- Ensuring that the Trust IT systems are secure and protected in line with the DFE Cyber security standards for schools and colleges.
- Ensure file storage is in line with the DfE Servers and storage standards for schools and colleges
- Conducting security checks and monitoring Trust IT systems on a regular basis.
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files.
- Maintaining block and allow lists for staff and students, ensuring consistency across all schools.

This list is not intended to be exhaustive.

4.6 All staff, volunteers, contractors and agency staff

All staff need to be aware of reporting mechanisms for safeguarding and technical concerns. They should report if:

- they witness or suspect unsuitable material has been accessed
- they can access unsuitable material
- they are teaching topics which could create unusual activity on the filtering logs
- there is failure in the software or abuse of the system
- there are perceived unreasonable restrictions that affect teaching and learning or administrative tasks
- they notice abbreviations or misspellings that allow access to restricted material

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's IT systems and the internet (Appendix 2) and ensuring that students follow the Trust terms on acceptable use (Appendix 1).
- Working with the DSL to ensure that any online safety incidents are logged (see Appendix 4) and dealt with appropriately in line with this policy.
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the 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'

- Understand the unique risks associated with online safety and be confident that they have the relevant knowledge and up to date capability required to keep children safe whilst they are online at school.
- Can recognise the additional risks that children with SEN and disabilities (SEND) face online, for example, from online bullying, grooming and radicalisation and are confident they have the ability to support SEND children to stay safe online.

This list is not intended to be exhaustive.

4.7 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's IT systems and internet (Appendix 1)

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

- UK Safer Internet Centre: https://saferinternet.org.uk/guide-and-resource
- Childnet International: https://www.childnet.com/parents-and-carers
- Keeping Children Safe Online - https://www.gov.uk/government/publications/coronavirus-covid-19-keeping-children-safe-online
- Safe Remote Learning - Safeguarding and remote education during coronavirus (COVID-19)

4.8 Visitors and members of the community

Visitors and members of the community who use the Trust's IT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (Appendix 2).

5.0 Preventative Action

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

- **Education** – School's preventative curriculums help pupils understand how to stay safe online and why certain content is unacceptable
- **Prevention** – All staff are vigilant and don't rely on technical monitoring
- **Reaction** – All staff should address unacceptable and unsafe behaviour and the DSL should investigate any online safeguarding incidents
- **Reporting and monitoring** – Leaders should review reports …so that strategies are put in place to ensure safe use of technology in our schools

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

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

6.0 Educating Students About Online Safety

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

In Key Stage 1, students will be taught to:

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

In Key Stage 2, students will be taught to:

- Use technology safely, respectfully, and responsibly
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact

In Key Stage 3, students will be taught to:

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

In Key Stage 4, students will be taught:

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

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

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

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

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

7.0 Educating Parents/Carers about Online Safety

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

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.

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

8.0 Harmful Online Challenges and Online Hoaxes

A hoax is a deliberate lie designed to seem truthful, and online challenges generally involve users recording themselves taking a challenge, and then distributing the video through social media channels, inspiring or daring others to repeat the challenge.

We are aware there are many children and young adults who struggle to identify harmful online challenges and online hoaxes.

DSLs together with the IT service will undertake a case-by-case assessment, establishing the scale and nature of the possible risk to our children and young people, including considering if the risk is national, local, or school related.

Where the assessment finds an online challenge to be putting pupils at risk of harm, e.g. it encourages children to participate in age-inappropriate activities that could increase safeguarding risks or become a child protection concern, they will ensure that the challenge is directly addressed to the relevant pupils, e.g. those within a particular age range that is directly affected or even to individual children at risk where appropriate.

We will provide appropriate guidance and which audiences this needs to go to following each assessment.

9.0 Cyber-bullying

Definition:

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

9.1 Preventing and addressing cyber-bullying

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

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

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

All staff, board members and volunteers (where appropriate) receive training on cyber-bullying, its impact, and ways to support students, as part of safeguarding training (see section 15 for more detail).

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

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

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

9.2 Examining electronic devices

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

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

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the school rules

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

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
- Report it to the police*

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

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

- The DfE's latest guidance on screening, searching and confiscation
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- The school's COVID-19 risk assessment

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

10.0 Acceptable Use of the Internet in School

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

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

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

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

10.1 Personal use of social media

10.1.1 Employees must not identify themselves as employees of the Trust in their personal web space. This is to prevent information on these sites from being linked with the Trust and to safeguard the privacy of staff members, particularly those involved in providing sensitive frontline services.

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

10.1.3 Employees must not have any contact with pupils' family members through personal social media if that contact is likely to constitute a conflict of interest or call into question their objectivity.

10.1.4 If employees wish to communicate with pupils through social media sites or to enable pupils to keep in touch with one another, they can only do so with the approval of the Trust and through official Trust sites created according to the requirements specified in section 11.

10.1.5 Employees must decline 'friend requests' from pupils they receive in their personal social media accounts. Instead, if they receive such requests from pupils of any school who are not family members, they may discuss these in general terms in class where the pupils attend the school and signpost pupils to become 'friends' of the official school site if there is one.

10.1.6 Information employees have access to as part of their employment, including personal information about pupils and their family members, colleagues, and other parties and Trust corporate information must not be discussed on their personal web space.

10.1.7 Photographs, videos, or any other types of images of pupils and their families or images depicting employees wearing clothing with school logos on must not be published on personal web space.

10.1.8 Trust/school email addresses and other official contact details must not be used for setting up personal social media accounts or to communicate through such media.

10.1.9 The Trust only permits limited personal use of social media during designated break points. However, employees are expected to devote their contracted hours of work to their professional duties, and, in practice, personal use of the internet should not be in the Trust's time. This is subject to such use:

- Not depriving pupils of the use of the equipment and/or
- Not interfering with the proper performance of employee's duties

10.1.10 Caution is advised when inviting work colleagues to be 'friends' in personal social networking sites. Social networking sites blur the line between work and personal lives, and it may be difficult to maintain professional relationships, or it might be just too embarrassing if too much personal information is known in the workplace.

10.1.11 Employees are advised that they set the privacy levels of their personal sites as strictly as they can and to opt out of public listings on social networking sites to protect their own privacy. Employees should keep their passwords confidential, change them often and be careful about what is posted online. It is not appropriate to reveal home addresses, telephone numbers and other personal information. It is a good idea to use a separate email address just for social networking so that any other contact details are not given away.

10.2 Using social media on behalf of the Trust

10.2.1 Employees can only use official Trust sites for communicating with pupils or to enable pupils to communicate with one another.

10.2.2 Employees should seek permission from the Headteacher before creating an official Trust related site explaining their business reasons for doing so.

10.2.3 Any official Trust sites created must not breach the terms and conditions of social media service providers, particularly regarding minimum age requirements.

10.2.4 Employees must always act in the best interests of children and young people when creating, participating in or contributing content to social media sites.

10.2.5 If you are contacted for comments about the Trust for publication anywhere, including in any **social media outlet please direct the enquiry to the Headteacher**.

10.3 Use of Trust IT

10.3.1 Staff who use the Trust's IT and communication systems:

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

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

10.4 Email and communications systems usage

10.4.1 The following uses of IT are prohibited, may amount to gross misconduct, and could result in dismissal. Please see the Disciplinary Policy for further guidance.

- To make, to gain access to, or for the publication and distribution of inappropriate sexual material, including text and/or images, or other material that may deprave or corrupt those likely to read or see it
- To make, to gain access to, and/or for the publication and distribution of material promoting homophobia or racial or religious hatred
- For the purpose of bullying or harassment, or for or in connection with discrimination on the grounds of gender, race, religion, disability, age or sexual orientation
- For the publication and/or distribution of libellous statements or material which defames or degrades others
- For the publication of material that brings the Trust/school or its pupils or employees into disrepute
- For the publication and distribution of personal data without authorisation
- Where the content of the email correspondence is unlawful
- To participate in on-line gambling
- Where the use infringes copyright law
- To gain unauthorised access to internal or external computer systems (commonly known as hacking)

- To create or deliberately distribute IT or communications systems viruses
- To record or monitor telephone or email communications without the express approval of the Trust. In no case will such recording, or monitoring be permitted unless it has been established that such action is in full compliance will the relevant legislation i.e. the Regulation of Investigatory Powers Act 2000.
- To participate in "chain" e-mail correspondence
- In pursuance of personal business or financial interests or political activities (excluding the legitimate activities of recognised trade unions).

10.5 Monitoring

10.5.1 The Trust (where authorised by the Headteacher) reserves the right to monitor usage of its internet and email services without prior notification or authorisation from users.

10.5.2 Case example: A recent European Court of Human Rights case ruled that an employer was legitimately entitled to access an employee's social media messenger account. This was because the messages had been sent during working hours, from a work account and on a work device. Therefore, users of the Trust's email and internet services should have no expectation of privacy in anything they create, store, send or receive using the Trust's IT system. As such employees should not use the school's IT resources or communication systems for any matters that are private and confidential.

10.6 Breaches of the policy

10.6.1 Any breach of this policy will be fully investigated and may lead to disciplinary action being taken against the employee/s involved in line with the Trust's Disciplinary Policy and Procedure.

10.6.2 A breach of this policy leading to breaches of confidentiality, or defamation or damage to the reputation of the Trust/school or any illegal act/s that render the Trust/school liable to third parties may result in disciplinary action or dismissal.

10.6.3 Contracted providers of the Trust's services must inform the Trust immediately if they become aware of any breaches of this policy so that appropriate action can be taken to protect confidential information and limit damage to the reputation of the Trust.

10.6.4 Under the Regulation of Investigatory Powers Act (2000) the Trust can exercise the right to monitor the use of the Trust's/school's information systems and internet access where it is believed that unauthorised use may be taking place, to ensure compliance with regulatory practices, to ensure standards of service are maintained, to prevent or detect crime, to protect the communications system and to pick up messages if someone is away from school.

10.6.5 In certain circumstances the Trust will be obliged to inform the Local Authority Designated Officer (LADO) and/or police of any activity where there are concerns that it may constitute a safeguarding issue or potentially involve illegal activity.

11.0 Students Using Mobile Devices in School

11.1 Trust schools may have different approaches to use of mobile devices in schools which should be reflected in the school's Positive Learning Strategy or Behaviour Protocol.

11.2 Students may bring mobile devices into school, but are not permitted to use them during:

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

Any use of mobile devices in Trust schools by students must be in line with the acceptable use agreement (see Appendix 1).

11.3 Any breach of the acceptable use agreement by a student may trigger disciplinary action in line with the Trust Behaviour Policy and school protocol, which may result in confiscation of their device.

12.0 Staff Using Work Devices Outside School

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

12.2 Staff must ensure that their work device is secure and password-protected, preferably encrypted where possible and practical, and that they do not share their password with others. Any USB, disks or portable hard drives devices containing Trust or school data must be encrypted/password protected.

12.3 Staff must take all reasonable steps to ensure the security of their work device when using it outside school. For example, but not limited to:

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

13.0 Insurance Requirements for Work IT Equipment and Mobile Phones

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

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

13.2 Work devices must be used solely for work activities.

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

14.0 How the Trust will Respond to Issues of Misuse

14.1 Where a student misuses the Trust's IT systems or internet, we will follow the procedures set out in the Trust Behaviour Policy and school protocol. The action taken will depend on the individual circumstances, nature, and seriousness of the specific incident, and will be proportionate.

14.2 Where a staff member misuses the Trust's IT systems or the internet or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures. The action taken will depend on the individual circumstances, nature, and seriousness of the specific incident.

14.3 The Trust will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

14.4 Any incidents which result in the unauthorised access, processing or sharing of personal data this will be considered a data breach under the Trust GDPR Data Protection and FOI Policy and must be notified immediately to the Cluster Business Manager.

15.0 Training

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

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

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

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

Training will also help staff:

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

15.3 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.

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

15.5 Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our Child Protection and Safeguarding policy.

16.0 Monitoring Arrangements

16.1 The DSL or Deputies will log behaviour and safeguarding issues related to online safety, using CPOMs.

17.0 Review

This policy will be reviewed annually.

The review will be supported by an annual risk assessment and information gathered by the external safeguarding reviews which considers and reflects the risks pupils face online. This is important because technology, and the risks and harms related to it, evolve, and change rapidly.

Appendix 1: Acceptable Use Agreement (Students and Parents/Carers)

<table>
<tr><th colspan="4">Beckfoot Trust Acceptable Use Agreement IT Systems and Internet</th></tr>
<tr><td>Name of Student:</td><td></td><td>Tutor/Reg Group:</td><td></td></tr>
<tr><td colspan="4">When using the Trust's IT systems and accessing the internet in Trust schools, I will not:
Use them for a non-educational purpose
Use them without a teacher being present, or without a teacher's permission
Access any inappropriate websites
Access social networking sites (unless my teacher has expressly allowed this as part of a learning activity)
Use chat rooms
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 my password with others or log in to the Trust or school's network using someone else's details
Give my personal information (including my name, address, or telephone number) to anyone without the permission of my teacher or parent/carer
Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision
If I bring a personal mobile phone or other personal electronic device into a Trust school:
I will not use it during lessons, tutor group time, clubs or other activities organised by the 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 agree that the Trust will monitor the websites I visit.
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's IT systems and internet responsibly.</td></tr>
<tr><td colspan="2">Signed (Student):</td><td colspan="2">Date:</td></tr>
<tr><td colspan="4">Parent/Carer agreement: I agree that my child can use the school's IT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for Students using the school's IT systems and internet, and for using personal electronic devices in schools and will make sure my child understands these.</td></tr>
<tr><td colspan="2">Signed (Parent/carer):</td><td colspan="2">Date:</td></tr>
</table>

Appendix 2: Acceptable Use Agreement Staff/Board & LSC Members/ Volunteers and Visitors

Beckfoot Trust - Acceptable Use Agreement IT Systems and Internet			
Name and Role		**School:**	

When using the Trust's IT systems and accessing the internet in the Trust, or outside 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
- Use them in any way which could harm the Trust'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
- Share my password with others or log in to the Trust's network using someone else's details

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

I agree that the Trust will monitor the websites I visit.

I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the Trust GDPR Data Protection and FOI policy.

I will let the Designated Safeguarding Lead (DSL) and IT manager know if a student 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 IT systems and internet responsibly and ensure that students in my care do so too.

Signed:	**Date:**