# ONLINE SAFETY POLICY

| | | | |
|---|---|---|---|
| Version | | 3.0 | |
| Date | | September 2019 | |
| Approved by Board of Directors | | 26/9/19 | |
| Version | Date | Description | Revision author |
| 1.0 | 03/01/2018 | Trust Version Created | FMW |
| 2.0 | 13/04/2018 | Social media policy included | GAD |
| 2.1 | 17/09/2018 | Minor amendment to link | AMV |
| 3.0 | 01/09/2019 | Amendment: 3.4 – Reword of 2 bullet points<br><br>Addition: 3.5 – understanding risks associated with online safety | GAD |

# Contents

# 1. Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of Students, staff, volunteers and Board members
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

# 2. Legislation and guidance

This policy is based on the Department for Education's statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on preventing and tackling bullying and searching, screening and confiscation. It also refers to the Department'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 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.

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

# 3. Roles and responsibilities

### 3.1 The Trust Board

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

The Trust Board will co-ordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

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 and Local Trust school ICT systems and the internet (appendix 2)

### 3.2 The headteacher

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

### 3.3 The designated safeguarding lead

Details of the local Trust School designated safeguarding lead (DSL) and deputies are set out in the local school version of the Trust Child Protection and Safeguarding Policy.

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, ICT manager and other staff, as necessary, to address any online safety issues or incidents
- Ensuring 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 logged and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety (appendix 3 contains a 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 school to the headteacher and/or Trust Board

This list is not intended to be exhaustive.

### 3.4 Local School ICT Management

The Associate Director ICT is responsible for:

- Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep Students safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the local Trust School ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting security checks and monitoring local Trust School ICT systems on a regular 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 4) and managed appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are managed appropriately in line with the school behaviour policy

This list is not intended to be exhaustive.

### 3.5 All Trust and local Trust school staff, Volunteers, Contractors and Agency Staff

All Trust and local Trust school 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 and local Trust School ICT 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
- 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.

### 3.6 Parents

Parents 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 and local Trust school's ICT systems and internet (appendix 1)

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

- What are the issues?, UK Safer Internet Centre: https://www.saferinternet.org.uk/advice-centre/parents-and-carers/what-are-issues
- Hot topics, Childnet International: http://www.childnet.com/parents-and-carers/hot-topics
- Parent factsheet, Childnet International: https://www.childnet.com/parents-and-carers

### 3.7 Visitors and members of the community

Visitors and members of the community who use the Trust or local Trust school's ICT 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).

# 4. 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

Students in **Key Stage 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

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

Students in **Key Stage 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

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.

# 5. Educating parents about online safety

Trust schools will raise parents' awareness of internet safety in various ways e.g. parents' evenings, letters, news items etc. through the Trust or local Trust school website or communication systems e.g. MyEd App, SIMS Learning Gateway etc.

If parents 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.

This policy will also be shared with parents on the Trust and Trust School Websites.

Concerns or queries about this policy can be raised with any member of staff or the headteacher.

# 6. Cyber-bullying

### 6.1 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.)

### 6.2 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 11 for more detail).

The school also sends information/leaflets on cyber-bullying to parents 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.

### 6.3 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

Any searching of Students will be carried out in line with the DfE's latest guidance on screening, searching and confiscation.

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

# 7. 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 and local Trust school ICT 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 and local 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 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.

**7.1 Personal Use of Social Media**

7.1.1 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.

7.1.2 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.

7.1.3 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.

7.1.4 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 9.

7.1.5 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.

7.1.6 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.

7.1.7 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.

7.1.8 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.

7.1.9 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 employees duties

7.1.10 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 work place.

7.1.11 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.

**7.2 Using Social Media on Behalf of the Trust**

7.2.1 Employees can only use official Trust/school sites for communicating with pupils or to enable

pupils to communicate with one another.

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

7.2.3 Any official Trust/school sites created must not breach the terms and conditions of social media service providers, particularly with regard to minimum age requirements.

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

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

**7.3 Use of School ICT**

7.3.1 Staff who use the Trust's ICT 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 ICT Co-ordinator 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/school's ICT systems

Must report to the Headteacher or designated safeguarding officer any vulnerabilities affecting child protection in the Trust's/school's ICT and communications systems

Must not install software on the Trust's/school's equipment unless authorised by the school's ICT Co-ordinator

Must comply with any ICT 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

7.3.2 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.

**7.4 Email and Communications Systems Usage**

7.4.1 The following uses of ICT 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 ICT 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

1. To participate in “chain” e-mail correspondence
2. In pursuance of personal business or financial interests or political activities (excluding the legitimate activities of recognised trade unions)

**7.5 Monitoring**

7.5.1 The Trust’s/school’s IT department (where authorised by the Headteacher) reserves the right to monitor usage of its internet and email services without prior notification or authorisation from users.

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.

7.5.2 Therefore Users of the Trust’s/school’s email and internet services should have no expectation of privacy in anything they create, store, send or receive using the Trust’s/school’s ICT system. As such employees should not use the schools IT resources or communication systems for any matters that are private and confidential.

**7.6 Breaches of the Policy**

7.6.1 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.

7.6.2 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.

7.6.3 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.

7.6.4 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.

7.6.5 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.

# 8. Students using mobile devices in school

Trust schools may have different approaches to use of mobile devices in schools and should be reflected in the local Trust school’s Positive Learning Strategy or Behaviour Policy.

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 Local Trust schools

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

Any breach of the acceptable use agreement by a Student may trigger disciplinary action in line with the local Trust school’s Behaviour Policy, which may result in the confiscation of their device.

# 9. Staff using work devices outside school

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

Staff must ensure that their work device is secure and password-protected, and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work device when using it outside school e.g. not connecting to an unprotected WIFI connection and where the screen may be visible by others when accessing personal data e.g. student and staff records. Any USB, disks or portable hard drives devices containing Trust or local Trust school data must be encrypted/password protected.

# 10. Insurance Requirements for work IT equipment and mobile phones

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 & 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 local Trust school ICT or Business manager.

Work devices must be used solely for work activities.

Loss or theft of any work equipment must be reported to the police immediately and local Trust school ICT or Business Manager immediately. Full details of the loss or theft will be required together with the crime reference number for insurance purposes.

# 11. How the Trust or Local Trust schools will respond to issues of misuse

Where a Student misuses the Trust or Trust local ICT systems or internet, we will follow the procedures set out in the local Trust school 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 or local 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 the staff disciplinary procedures. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

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

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

# 12. Training

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, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

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

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

Volunteers will receive appropriate training and updates, if applicable.

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

# 13. Monitoring arrangements

The local Trust school DSL or deputies will log behaviour and safeguarding issues related to online safety, using their preferred recording system e.g. SIMS/CPOMs. An example incident report log can be found in appendix 4 for use where schools do not have a reporting system in place.

This policy will be reviewed annually by the Trust Compliance Officer.

# 13. Links with other policies

This Online Safety Policy is linked to our:

- Trust Child protection and Safeguarding Policy
- Local Trust school Behaviour policy
- Trust Staff Discipline, Conduct and Grievance (includes Statement of Procedures for dealing with allegations of abuse against staff)
- Trust GDPR, Data Protection and FOI Policy
- Trust Staff, Student and Visitor/Volunteer Privacy Notices
- Trust Complaints Procedure
- Trust Code of Conduct

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

Beckfoot Trust

| (Insert School Name) - Acceptable Use Agreement ICT Systems and Internet | | | |
|---|---|---|---|
| **Name of Student:** | | **Tutor/Reg Group** | |

**When using the Trust or Local Trust school's ICT systems and accessing the internet in within 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 Local Trust 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 or Local Trust school 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 or Local Trust school's ICT systems and internet responsibly.

| **Signed (Student):** | **Date:** |
|---|---|

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

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

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

| Beckfoot Trust - Acceptable Use Agreement ICT Systems and Internet | | | |
|---|---|---|---|
| **Name of Staff Member/ Board and LSC Member/Volunteer/Visitor:** | | **School** | |

When using the Trust or Local Trust school's ICT systems and accessing the internet in Trust or Local Trust school, 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 or Local 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
- Share my password with others or log in to the Trust or Local Trust school's network using someone else's details

I will only use the Trust or Local Trust school's ICT systems and access the internet in Local 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 or Local Trust school 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 ICT 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 and Local Trust school ICT systems and internet responsibly, and ensure that Students in my care do so too.

| **Signed (staff member/Board and LSC Member/Volunteer/Visitor):** | **Date:** |
|---|---|

## Appendix 3: Online Safety Training Needs – Self-Audit

This form is intended to be used to assess your Online Safety Training Needs. Please complete this form and discuss the results with your line manager to enable appropriate support and guidance to be arranged.

| Online safety training needs audit | |
|---|---|
| **Name of staff member/volunteer:** | **Date:** |
| Do you know the name of the person who has lead responsibility for online safety in your school? | |
| Do you know what you must do if a Student approaches you with a concern or issue? | |
| Are you familiar with the Trust Acceptable Use Agreement for Staff, Volunteers, Board members and Visitors? | |
| Are you familiar with the Trust Acceptable Use Agreement for Students and Parents? | |
| Do you regularly change your password for accessing Trust and Local Trust school ICT systems? | |
| Are you familiar with the Trust and Local Trust school approach to tackling cyber-bullying? | |
| Are there any areas of online safety in which you would like training/further training? Please record them here. | |

**Appendix 4: Example Online Safety Incident Report Log**

| Online safety incident report log | | | | |
|---|---|---|---|---|
| **Date** | **Where the incident took place** | **Description of the incident** | **Action taken** | **Name and signature of staff member recording the incident** |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

Digital data will be coded, encrypted or password-protected, both on a local hard drive and on a network drive that is regularly backed up off-site.

Where data is saved on removable storage or a portable device, the device will be kept in a locked filing cabinet, drawer or safe when not in use.

Memory sticks will not be used to hold personal information unless they are password-protected and fully encrypted.

All electronic devices are password-protected to protect the information on the device in case of theft.

Where possible, the school enables electronic devices to allow the remote blocking or deletion of data in case of theft.

Staff and governors will not use their personal laptops or computers for school purposes.

All necessary members of staff are provided with their own secure login and password, and every computer regularly prompts users to change their password.

Emails containing sensitive or confidential information are password-protected if there are unsecure servers between the sender and the recipient.

Circular emails to parent/carer (person with legal responsibility)/legal guardings are sent blind carbon copy (bcc), so email addresses are not disclosed to other recipients.

When sending confidential information by fax, staff will always check that the recipient is correct before sending.

Where personal information that could be considered private or confidential is taken off the premises, either in electronic or paper format, staff will take extra care to follow the same procedures for security, e.g. keeping devices under lock and key. The person taking the information from the school premises accepts full responsibility for the security of the data.

Before sharing data, all staff members will ensure:

They are allowed to share it.

That adequate security is in place to protect it.

Who will receive the data has been outlined in a privacy notice.

Under no circumstances are visitors allowed access to confidential or personal information. Visitors to areas of the school containing sensitive information are supervised at all times.

The physical security of the school's buildings and storage systems, and access to them, is reviewed on a termly basis. If an increased risk in vandalism/burglary/theft is identified, extra measures to secure data storage will be put in place.

Beckfoot Trust takes its duties under the GDPR seriously and any unauthorised disclosure may result in disciplinary action.

The school business manager (SBM) is responsible for continuity and recovery measures are in place to ensure the security of protected data.

Publication of information

Beckfoot Trust publishes a publication scheme on its website outlining classes of information that will be made routinely available, including:

Policies and procedures

Minutes of meetings

Annual reports

Financial information

Classes of information specified in the publication scheme are made available quickly and easily on request.

Beckfoot Trust will not publish any personal information, including photos, on its website without the permission of the affected individual.

When uploading information to the school website, staff are considerate of any metadata or deletions which could be accessed in documents and images on the site.