Beeston Primary School

Online Safety Policy

Date agreed by Governing Body	January 2024
Review date	January 2025
Responsible for this policy	Ashleigh Farrington

Checklist	
Has the school an Online Safety Policy?	✓
Date of last update	May 2023
Is the policy available for staff and parents and is also online	✓
The responsible member of the Senior Leadership Team is	Mrs S. Knowles
The responsible member of the Governing Body is	Miss L. Hegarty
The Designated Child Protection Co-Ordinators are	Mrs S. Knowles, Mr N. Edensor, Mrs R. Wilkinson, Mrs L. Jackson, Mrs M. Whitaker
The Online Safety Co-Ordinators are	Mrs S. Knowles, Miss A. Farrington

Contents

1. Aims

Our 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 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, such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, 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 scams

2. 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 schools on:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- Relationships and sex education –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.

3. Roles and responsibilities

3.1 The governing board

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

The governing board 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 board 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 board will co-ordinate regular meetings 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 board should ensure children are taught how to keep themselves and others safe, including keeping safe online.

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

The governor who oversees online safety is Miss. L. Hegarty

All governors will:

- Ensure they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 3)
- Ensure that online safety is a running and interrelated theme while devising and implementing their whole-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

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 school's designated safeguarding lead (DSL) are set out in our child protection and safeguarding policy, as well as relevant job descriptions.

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 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 school devices and school networks
- Working with the ICT manager to make sure the appropriate systems and processes are in place
- Working with the headteacher, ICT 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's child protection policy
- Ensuring that any online safety incidents are logged on CPOMS 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 4 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 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.

3.4 The ICT manager

The ICT manager is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems on school devices and 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 school, including terrorist and extremist material
- Ensuring that the 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 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 on CPOMs 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

This list is not intended to be exhaustive.

3.5 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 school's ICT systems and the internet (appendix 3), and ensuring that pupils follow the school's terms on acceptable use (appendices 1 and 2)
- 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 recording on our Sharepoint log file and emailing the DSL and ICT manager.
- Following the correct procedures by submitting a request ticket to the helpdesk 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 on CPOMS 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
- Ensuring all digital communication with parents/carers/students is of a professional manner and be carried out using official school system
- 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'
- Treat equipment with reasonable care. If a device is stolen, report it to the police for a crime reference number and to the computing lead as soon as possible.

This list is not intended to be exhaustive.

3.6 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 school's ICT systems and internet (appendices 1 and 2)

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
- Hot topics – Childnet International
- Parent resource sheet – Childnet International

3.7 Visitors and members of the community

Visitors and members of the community who use the 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 3).

4. Educating pupils about online safety

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

The text below is taken from the National Curriculum computing programmes of study and guidance on relationships education, relationships and sex education (RSE) and health education.

All schools have to teach:

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

In **Key Stage (KS) 1**, pupils 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 in **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

By the **end of primary school**, 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

We ensure that the school meets the needs of all, taking account of gender, ethnicity, culture, religion, language, sexual orientation, age, ability, disability and social circumstances. It is important that in school we meet the diverse needs of pupils to ensure inclusion for all and that all pupils are prepared for full participation in a multi-ethnic society. We measure and assess the impact through meetings with our SEND co-ordinator and individual teachers to ensure all children have equal access to success in this subject.

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.

5. Educating parents/carers about online safety

Technology advancements are rapid. Many parents and carers have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring/regulation of the children's online behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond. It is a parent/carers responsibility to monitor their child's online use outside of school.

The school will therefore seek to provide information and awareness to parents and carers through:

- Letters, newsletters, web site pages
- Parents/Carers evenings/sessions
- Events/campaigns e.g. Safer Internet Day
- Reference to the relevant web sites/publications

A page can be found on our school website under 'Safeguarding' as an information access point, detailing up to date online safety issues that may concern their children. The school will let parents/carers know:

- What systems the school uses to filter and monitor online use
- What their children are being asked to do online, including the sites they will be asked to access and who from the 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 DSL.

6. Technical: Infrastructure, filtering and monitoring

The school will be responsible for ensuring that the school network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their online safety responsibilities:

- If staff or pupils discover unsuitable sites, the URL (address), time and content shall be logged by the teacher, reported to the Online Safety Coordinator or Wavenet engineer, who will check the content and request the site be blocked.
- All internet access is monitored by the 'Netsweeper' filtering system which is updated regularly to stay current.
- Any searches, which do not conform to the acceptable use policy, will be reported via email to the DSL and Computing Leader. This can then be actioned by a member of staff and recorded for evidence on CPOMS.
- The school has enhanced/differentiated user-level filtering for staff and students.
- Users (Years 2-6) will be provided with a username by Wavenet, who will keep an up to date record of users and their usernames. Users are responsible for the security of their username and password.
- Staff must always 'lock' the PC if they are going to leave it unattended.
- There will be regular reviews and audits of the safety and security of school technical systems.
- Servers, wireless systems and cabling must be securely located and physical access restricted.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data.
- The school infrastructure is protected by up to date virus software.
- Temporary access of "guests" (eg trainee teachers) onto the school systems through the provision of their own log in. Such users should abide by all elements of this policy.
- Staff are forbidden from downloading executable files and installing programmes on school devices. (Please consult an Wavenet engineer)
- Removable media (eg memory sticks / CDs / DVDs) may be used by users on school devices, ensuring any data relating to named children must be encrypted if it is to be taken off site. OneDrive Cloud storage should be considered as a safer option.

7. Cyber-bullying

7.1 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 1 person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.)

7.2 Preventing and addressing cyber-bullying

This policy should be read in line with our school Anti Bullying Policy which references:

Bullying On-line and Social Media.

- Most of the inappropriate use of the internet is done from home or on students' mobile devices during evenings, weekends and school holidays.
- Staff at school have no jurisdiction to deal with this, and cannot investigate it.
- The responsibility for monitoring a child's use of social media, or indeed the internet in general, must lie with parents/guardians.
- School can offer advice to parents on keeping their child safe online or how to report bullying incidents.

Parents have a wide range of resources accessible on the school website, accessible from our main Safeguarding page, to provide support on how to deal with issues arising at home and routes for reporting inappropriate online content.

The Department for Education has released a document that aims to help parents better understand the issues and offers advice about many aspects of cyberbullying. Cyberbullying: Advice for Parents/Carers.

7.3 Examining electronic devices

The headteacher, and any member of staff authorised to do so by the headteacher, as set out in our behaviour policy, can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

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

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 Senior Leadership Team.
- Explain to the pupil why they are being searched, how the search will happen, and give them the opportunity to ask questions about it
- Seek the pupil's co-operation

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on an electronic 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 an electronic device, the staff member should reasonably suspect that the device has, or could be used to:

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

If inappropriate material is found on the device, it is up to the Senior Leadership Team 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 if there is a good reason to erase data or files from a device, staff members will consider if 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 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/carer 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
- Confiscate the device and report the incident to the DSL (or equivalent) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on screening, searching and confiscation and the UK Council for Internet Safety (UKCIS) 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 guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- Our behaviour policy

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

7.4 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 Bard.

Beeston Primary School 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.

Beeston Primary School will treat any use of AI to bully pupils in line with our anti-bullying and Positive behaviour policies.

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 school.

8. Acceptable use of the internet in school

All pupils, parents/carers, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendices A, 1, 2 and 3). Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

Use of the 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 comply with the above and restrict access through filtering systems where appropriate.

More information is set out in the acceptable use agreements in appendices A, 1, 2 and 3.

9. Mobile devices in school

Year 5 and 6 pupils, by permission of the Headteacher, can bring mobile phones onto the school site where it is seen by the school and parents as a safety/precautionary use. These are handed into the class teacher on arrival and locked away. Whilst on school grounds, pupil's mobile phones must be turned off at all times. If a child is found using their phone on school grounds, staff have the right to confiscate it and will no longer be allowed to bring their phone to school. Parents or carers will be informed of this and will have to collect the phone from the school office. Children should not wear smart watches to school.

- The sending of abusive or inappropriate text messages is forbidden, including nude and semi nude images, pornography or other explicit content.
- Staff should use the school phone to contact parents. Where this is not possible they must withhold their caller ID using the phone settings.
- Staff are required to switch off their mobile phones before entering the school building and should be stored safely away in their locker. Staff are only permitted to access and use their mobile phones, at break and lunchtime, in a 'mobile safe zone;' these are located in the staff room and Senior Leadership Team offices.
- On entering school premises, pupils, visitors and parents will be requested to switch off mobile phones.
- ONLY school equipment should be used to record classroom activities.

- Photographs and recordings can only be transferred to and stored on a school computer before printing. Images must not be transferred to unsecured external storage devices (e.g. USB sticks, external hard drives).
- Adults, including Staff and Parents, cannot use mobile phones on school trips to take pictures of the children.
- School mobile phones (no camera function) for use in case of emergency (eg. bus breakdown) are available for use on educational visits, including weekly swimming lessons.

Any use of mobile devices in school must be in line with the acceptable use agreement (see appendices 1 and 2).

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

This policy has been updated in line with 'Guidance for Safer Working Practice, 2022'.

10. Staff using work devices outside 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 are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)
- 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
- Lock devices 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 school's terms of acceptable use, as set out in appendix 3.

Work devices must be used solely for work activities.

If staff have any concerns over the security of their device, they must seek advice from the ICT manager/Onsite technician.

11. How the school will respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our policies on behaviour and Internet acceptable use. 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 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 / staff code of conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

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

12. Use of digital photo and video images

The development of digital imaging technologies allows staff and students instant use of images. However, staff, parents/carers and students need to be aware of the risks associated with publishing digital images on the internet and comply with The General Data Protection Regulation.

Using images of students for publicity purposes requires the age-appropriate consent of the individual concerned and their legal guardians (now collected digitally using Microsoft Forms and stored on the server). Images should not be displayed on websites, in publications or in a public place without such consent. The definition of a public place includes areas where visitors to the school or service provision have access. Consent to use images can be withdrawn at any time, without giving a reason, and in such cases, staff must make every effort to remove/destroy these images wherever they have been published.

Staff will ensure that images are held only for as long as necessary for the purpose. The recommendation for images of children is that they should only be held for 2 years.

> *For further guidance on creating, displaying and storing images of students please refer to the Safer Working Practice Guidance (National Safer Recruitment Consortium 2022) as well as guidance from the Department for Education (Safeguarding Children in a Digital World) and CEOP (Child Exploitation and Online Protection).*

12.1 Photography and filming of children in school

The General Data Protection Regulation considers an image of a child to be personal data and does not permit such photos or videos to be sold, put on public display, the internet or uploaded to social media.

Parents do not need to comply with the General Data Protection Regulation if they are taking photographs or making a video recording of their **own child** for private use. Parents at Beeston Primary School are therefore permitted to take photographs or make video recordings of their **own child** at school events such as concerts and sports day. The recording or photography of other children would require parental consent. Without this consent the General Data Protection Regulation would be breached. This applies to both staff, parents and pupils.

- The Headteacher or a nominee will inform parent(s)/guardian(s) and others present at school events that photographs/videos may be taken on the basis that they are for private retention and not for publication in any manner explaining the importance of this for some children
- Staff should always use a school device to capture images.
- Photographs including students will be selected carefully and will comply with good practice guidance on the use of such images when being published online.
- Students' full names will not be used anywhere on the website or social media.
- Children's names will not be used alongside images, including in the media, without parental consent.

Written permission from parents or carers and verbal permission of pupils will be obtained before identifiable photographs of students are published on the school website/social media/school publications.

Staff should also be mindful of seeking the child's permission to include them in photography, respecting their digital footprint.

12.2 Photography of staff

Photographs and video images of school staff are classed as personal data under the terms of the General Data Protection Regulation. Therefore, using such images will require the consent of the staff member concerned. Parents are not permitted to photograph/film members of staff at Beeston Primary School without consent.

13. Communications

- Users must immediately report, to the Senior Leadership Team, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Any digital communication between staff and students or parents/carers must be professional in tone and content. Personal email addresses, text messaging or social media must not be used for these communications.
- Online services such as 'Class Dojo' may be used for staff to communicate on a professional basis with parents but any such communications must not refer to named children, other than those for whom the adult has parental responsibility.
- Students and staff may be provided with logins for school related sites and online services. It is their responsibility to use these services appropriately and in accordance with other parts of this policy.
- Personal information should not be posted on the school website or class blogs and only official email addresses should be used to identify members of staff.

13.1 Email

E-mail is a quick and easy method of communication, ensuring beneficial and appropriate usage is an important part of online safety:

- At present the children do not access the email accounts within their Microsoft tenancy. We have a group email address for the Junior Leadership team which is limited to send/receive from addresses within our tenancy. This is further managed by a member of staff during their meetings.

When email is being used within school:

- Pupils may only use approved e-mail accounts on the school system.
- Pupils accounts operate on an internal mail system.
- Pupils must immediately tell a teacher if they receive an offensive e-mail.
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- E-mails from unknown sources should be treated as suspicious and attachments not opened unless the author is known.
- The school should consider how e-mail from pupils to external bodies is presented and controlled.
- School will have access to check student mailboxes should they deem it necessary.
- Users should not sign up to any non-work-related online accounts using their school email address.

13.2 Social Networking

Social networking internet sites provide facilities to chat and exchange information online, such as: Twitter, Facebook, YouTube, comment streams on public websites and virtual world gaming sites. This online world is very different from the real one with the temptation to say and do things beyond usual face-to-face contact.

- At a pupil level, use of social networking sites in the school, is not allowed and will be blocked/filtered.

- At a staff level, Facebook will be accessed for uploading of photographs/comments to share home learning with families.
- Pupils and parents will be advised that the use of social network spaces outside school carries dangers and they should be acknowledging the minimum age recommended by that platform.
- Parents, pupils and staff will be advised of the dangers of discussing pupils, staff or the school on social networking sites.
- Whilst at school, children will be educated on how to use social media appropriately, however outside of school it is the responsibility of parents/carers to monitor their child's use. With regards to social media use, staff have no jurisdiction to deal with events that happen outside of school.

School staff should ensure that:

- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to the school or local authority
- Any communication received from children on any personal social media sites must be reported to the designated child protection lead. NB. Teachers will be able to message students using the Microsoft Education platform regarding their learning.
- It is not advisable to invite parents/carers to become your friends on social networking sites. There may be a conflict of interest, security and privacy issues, but where relationships are already established, staff should proceed with caution, being fully aware of the social media guidelines and the staff code of conduct.
- Staff should not accept any current pupil of any age, or any ex-pupil under the age of 18 as a friend, follower, subscriber or similar on any personal social media account.
- Staff should understand and check their privacy and security settings on social media profiles to limit who has access to their data. They may also want to consider how much personal information is included in online profiles

The use of social media for professional purposes:

- Staff should set up a distinct and dedicated social media site or account for educational purposes (eg. Mr Mc, TishyLishy etc).
- The URL or identity of the site should be notified to the Headteacher before access is permitted for anyone outside of the school.
- The content of any school-sanctioned social media site should be solely professional and should reflect well on the school. A link on the school website will indicate that the account is officially sanctioned by Beeston Primary School.

School social media:

- Staff will access the 'Beeston Primary School – Leeds' Facebook page through personal Facebook accounts, however, security settings have been put in place to ensure the page will only post under the group 'Beeston Primary School – Leeds' alias.
- Staff with access to the Facebook page will abide by an additional Acceptable Use agreement (Appendix 5).
- Care must be taken that any links to external sites from the account are appropriate and safe.

Any inappropriate comments or abuse of school-sanctioned social media should immediately be screen-shot for evidence, removed and reported to the Computing Leader and member of the Senior Leadership Team.

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).

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 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 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.

13. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety.

This policy will be reviewed every year by the Computing Leader At every review, the policy will be shared with the governing board. The review (such as the one available here) will be supported by an annual risk assessment that 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.

14. Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy
- Staff disciplinary procedures

- Data protection policy and privacy notices
- Complaints procedure
- ICT and internet acceptable use agreement

Appendix A: Acceptable use agreement letter

Beeston Primary School

Town Street, Leeds, LS11 8PN

"Promoting a love of learning"

Dear Parent/Carer,

RE: Responsible use of the Internet

As part of the pupil's curriculum enhancement and the development of ICT skills, Beeston Primary School is providing supervised access to the internet including email.

Although there have been concerns nationally about pupils having access to undesirable materials, we are taking positive steps to deal with this risk in school. Our school Interned access provider operates a filtering system that restricts access to inappropriate materials, and your child will be using the internet under supervision. Your child's activity on the internet will be monitored and reported to the Headteacher on a regular basis.

Whilst every effort is made to ensure that suitable restrictions are in place and working effectively to prevent children gaining access to inappropriate materials, neither the school nor the Council will be liable under any circumstances for any injury, distress, loss or damage to the pupil or the parents, which may arise directly or indirectly from the pupil's use of the internet facilities, the use of email, or from other pupils unauthorised use of those facilities or email.

The Council cannot be held responsible for the nature of content of materials accessed through the internet. The Council will not be liable under any circumstances for any damage arising from your child's use of the internet facilities.

Attached to this letter are the *'Rules of Responsible Internet Use'* that we operate at Beeston Primary School. Please read through them with your child and then complete the permission for internet access slip at the bottom of this letter and return to school.

Should you wish to discuss any aspects of the internet use please do not hesitate to contact the school office to arrange an appointment.

Yours Sincerely,

Mr N Edensor
Headteacher

Permission for Internet Access Slip

Name: _____ Class: _____

I have read the *'Rules of Responsible Internet Use'* with my child.

I give permission for my child to access the internet in line with the terms set out in this letter. I consent to the monitoring and auditing of my child's internet access.

Signed: _____ *(Parent/Carer)* Date: _____

Pupils Agreement

I agree to follow the *'Rules of Responsible Internet Use'*. I agree to the monitoring and auditing of my mail and internet access.

Signed: _____ Date: _____

Headteacher Mr. N. Edensor
Tel. No. 0113 2716978
www.beestonprimaryschool.co.uk
Part of the Leodis Schools Alliance

Appendix 1: EYFS and KS1 acceptable use agreement (pupils and parents/carers)

KS1 Computing Acceptable Use

To help me stay safe on a computer or iPad…

I will only use a computer or iPad when an adult tells me I can.

I will not share my username and password, or use those belonging to others.

I will tell an adult if I see something that upsets me.

I will only use activities that an adult has told/allowed me to use.

I will take care of the computer and other equipment.

I will make sure that I don't spoil other people's work.

I will ask for help from an adult if I am not sure what to do, or if I think I have done something wrong.

Appendix 2: KS2, KS3 and KS4 acceptable use agreement (pupils and parents/carers)

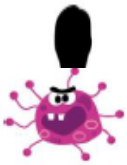
KS2 Computing Acceptable Use

To help me stay safe on a computer or iPad…

I will ask permission before using the Internet and use it for school purposes only.

I will never share my personal details, such as my full name, address or phone number with people I don't know.

I will not share my username and password, or use those belonging to others.



I will never meet up with someone I have met on the Internet, unless my parents or teachers say I can. In which case, I will do so in a public place and take an adult with me.

I will not purposefully open or download files which are inappropriate, illegal or may cause harm or distress to others.

I will not reply to a message that isn't kind, but will save it and show it to an adult.

I will tell an adult if something on the internet makes me or my friends unhappy.

I will treat equipment with care and tell an adult if something becomes broken.

I will only use polite language in online communication and searches.

I will not access, remove or alter other people's work without their permission or interfere with their computer while they are working.

Appendix 3: acceptable use agreement (staff, governors, volunteers and visitors)

Ref No: - _____

Staff Loan agreement

These items will be loaned to _____ for the duration of their employment at the school subject to the following terms and the schools ICT policy. All items must be returned to the school on ceasing to be employed at the school and during an extended planned absence.

1. The device is for the work related use of the named member of staff to which it is issued.
2. Only School related apps may be installed onto the device or any authorised software (further details to follow).
3. The device remains the property of the School throughout the loan period. The member of staff to which it is issued, will be required to take responsibility for its care and safe keeping.
4. All loan items are covered by the School's Insurance, when at home or school, providing it is not left unattended. Devices should never be left in a vehicle as they are NOT insured on our policy. School will look to reclaim any lost assets.
5. If left unattended the device should be in a locked room or secure area.
6. Due regard must be given to the security of the device if using other forms of transport.
7. In order to ensure the schools compliance with the Data Protection Act and to avoid breaches of confidentiality: under no circumstances should students be allowed to use the staff devices if not directly supervised by a member of staff. Staff should also be cautious when using the device away from school particularly with files which may contain personal student data.
8. Each member of staff will have a username and password which should be kept private to ensure the schools compliance with the Data Protection Act.
9. The device will be recalled from time to time for maintenance/ upgrade and monitoring.

Item	Serial Number/ ID	Signed Out Date	Returned Date

I have read and agree to the terms and conditions in this agreement.
I undertake to take due care of the device and return it when requested.

Signed:_____
Date:_____

This policy should be read in conjunction with the school's Safeguarding Policy and Procedures (including Child Protection). All our practice and activities must be consistent and in line with the Safeguarding Policy and Procedures noted above. Any deviations from these policies and procedures should be brought to the attention of the Headteacher so that the matter can be addressed.

Appendix 4: 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 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 school's acceptable use agreement for staff, volunteers, governors and visitors?	
Are you familiar with the school's acceptable use agreement for pupils and parents/carers?	
Are you familiar with the filtering and monitoring systems on the school's devices and networks?	
Do you understand your role and responsibilities in relation to filtering and monitoring?	
Do you regularly change your password for accessing the school's ICT systems?	
Are you familiar with the school's approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/further training?	

Appendix 5: Facebook Page Staff Guidelines

Beeston Primary School Facebook Page Staff Guidelines

- Staff should only post photos of children who have provided a 'Photo Permission' form.
- When photographing or videoing children for Facebook posts, children without photo permission should be cropped or edited out of photos before being posted on Facebook.
- Full names of children should not be mentioned in any posts or comments and never a photo and name of children.
- Staff should not identify their location whilst on school trips or off-site and posts should be made on return to school. (Residential private pages may post whilst away due to the privacy settings of the page).
- Posts containing photos of children should only be made using the school devices (iPad, laptop or desktop).
- Personal devices should **only** be used for informative posts containing no sensitive information eg. Child photos.
- Posts should celebrate children's achievements and should be of a positive nature.
- Please ensure you mention your year group within the post. (eg. Year 1… This week we have… etc)
- Staff must not post personal comments, videos or photos using the school's Facebook page.
- The Computing Subject Leaders will be responsible for page administration and maintenance, such as accepting comments and tags from external companies (eg. The Wonderdome).
- We will ensure that the settings remain in place to enable staff to post from within their personal accounts but appear externally as 'Beeston Primary School – Leeds'.
- Any concerns regarding the content of posts should be reported immediately to Computing Leaders and the Headteacher.

Name: _____

Signed: _____ Date: _____