Beeston Primary School

Online Safety Policy

Date agreed by Governing Body	05th May 2022
Review date	May 2023
Responsible for this policy	Ashleigh Farrington

Checklist	
Has the school an Online Safety Policy?	✓
Date of last update	May 2022
Is the policy is 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. Heggarty
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

1. Aims:

ICT in the 21st Century is seen as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults.

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- 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

This guidance applies to all staff, regardless of their capacity, based at Beeston Primary school. All staff are expected to adhere to this code of practice to ensure the safety of the students, young people and adults. Any member of staff found to be suspected of any breach of these guidelines may be subject to disciplinary action in accordance with the Schools Disciplinary Policy and Procedure.

2. Roles and Responsibilities

Governors:	Headteacher and Senior Leaders:
• Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. The role of the Online Safety Governor will include: ○ Meetings with the Online Safety Co-ordinator. ○ Monitoring of online safety incident logs. ○ Reporting to relevant Governors meetings. • Governors are responsible for ensuring the school partakes in annual safeguarding training including that of online safety.	• The Headteacher is responsible for ensuring the safety (including online safety) of members of the school community, though the day-to-day responsibility for online safety will be delegated to the Online Safety Co-ordinator. • The Headteacher/Senior Leaders are responsible for ensuring that the Online Safety Co-ordinators and other relevant staff receive suitable CPD to enable them to carry out their online safety roles and to train other colleagues, as relevant, on an annual basis. • The Headteacher/Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles. • The Senior Leadership team should be aware of the procedures to be followed in the event of a serious online safety allegation being made (Appendix A)

The Online Safety Co-ordinators:	Child Protection/ Safeguarding Designated Person:
• Takes day-to day-responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policy/documents. • Ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place (Appendix A). • Provides training and advice for staff. • Liaises with school technical staff. • Review logs of online safety incidents to inform future online safety developments. • Reports to Senior Leadership Team.	Child Protection/ Safeguarding Staff should be trained in online safety issues and be aware of the potential for serious child protection/ safeguarding issues to arise from: • Sharing of personal data • Access to illegal/inappropriate materials • Making/sharing/receiving inappropriate content • Inappropriate online contact with adults/strangers • Potential or actual incidents of grooming • Cyber-bullying • Radicalisation

Technical staff:
The Technical Support Staff and Computing Co-ordinator are responsible for ensuring: • That the school's technical infrastructure is secure and is not open to misuse or malicious attack. • That the school meets required online safety technical requirements and any Local Authority/other relevant body Online Safety Policy/Guidance that may apply. • That users may only access the networks and devices through a properly enforced password protection policy. • Content filtering is applied and updated on a regular basis in consultation with the online safety coordinator. • That they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant. • That the use of the network/ internet/ remote access/ email is regularly monitored (as far as is technically possible) in order that any misuse/attempted misuse can be reported to the Headteacher/Online safety Coordinator for investigation/ action/ sanction. • That a software audit is maintained and is available for any official body who require it for the purpose of copyright enforcement.

Teaching and Support Staff:
Teaching and Support Staff are responsible for ensuring that: • They have an up to date awareness of online safety matters and of the current school online safety policy and practices. • They will have an up to date knowledge of safeguarding issues that can put children at risk as harm, eg, the sharing of nude and semi-nude images/videos that can be signs of children at risk and radicalisation etc. • They have read, understood and signed the Staff Acceptable Use Agreement (Appendix D) • They report any suspected misuse or problem to the Online Safety Coordinator for investigation/action/sanction. • All digital communications with students/parents/carers should be on a professional level and only carried out using official school systems. • Online safety teaching is embedded in all aspects of the curriculum and other activities. • Students understand and follow the online safety and acceptable use policies. • KS2 students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations. • They monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities (where allowed) and implement current policies with regard to these devices.

- Processes are in place for dealing with any unsuitable material that is found in internet searches.
- Staff must ensure their passwords are secure and of a significant strength. These must not be shared with any member of staff or pupil.
- Staff must take reasonable care with all portable equipment. If a laptop is stolen, a report must be made to the police for a crime reference number and to the Computing Lead as soon as possible.
- Staff are responsible for ensuring their own use of ICT and social media is professional and appropriate at all times. Staff must be aware that their conduct online, both inside and outside of school, must not breach the school's code of conduct or professional expectations. Any such behaviours may be subject to disciplinary action.

Students:	**Parents/Carers:**
• Are responsible for using the school digital technology systems in accordance with the Student Acceptable Use Policy (Appendix C). • Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations (KS2). • Understand the importance of reporting abuse, misuse or access to inappropriate materials • Will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking/use of images, including sharing nude and semi-nude images and/or videos, making, sending and receiving other explicit images and videos, and on cyber-bullying. • Should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's online safety policy covers their actions out of school, if related to their membership of the school. • We will continue to utilise Teams as a learning platform. If accessing from home, pupils will follow the Remote	Parents/Carers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website and information about national/local online safety campaigns/literature. It is, however, down to parents and carers to keep their child safe online when not in school. Parents and carers will be encouraged to support the school in promoting good online practice and to follow guidelines on the appropriate use of: o Digital and video images taken at school events. o Social media. o Their children's personal devices in the school (where this is allowed). • We will continue to utilise Teams as a learning platform. If accessing from home, parents will ensure pupils follow the Remote Learning Acceptable Use document (appendix H)

Learning Acceptable Use document (appendix H)	

3. Online Safety-Education

Students
The education of students in online safety is an essential part of the school's online safety provision. Children and young people need the help and support of the school to recognise and avoid online risks and build their resilience. Online safety is delivered across the curriculum to help students understand these risks are now part of their everyday lives and to ensure they are always vigilant. We utilise Education for a Connected World to ensure broad, relevant and provide progression of the curriculum. It will: • Provide key online safety messages regularly, across the curriculum, reinforced as part of a planned programme of themed sessions (cyber safe afternoons). • Students should be helped to understand the need for the Student Acceptable Use Agreement (Appendix C and H) and encouraged to adopt safe and responsible use both within and outside school. • Staff should act as good role models in their use of digital technologies, the internet and mobile devices (including citation). • Where students are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit. In **Key Stage 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 2** will be taught to: • Use technology safely, respectfully and responsibly • Recognise acceptable and unacceptable behaviour (Including, but not limited to, Fake news and citation) • Identify a range of ways to report concerns about content and contact, Conduct and Commerce- considered the four main areas of risk *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*
- *How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know (RSE 2020)*

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.

Parents/Carers
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.

4. 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 AdEpt engineer, who will check the content and request the site be blocked.
- All internet access is monitored by the 'SonicWall' filtering system which is updated regularly to stay current.
- Any searches, which do not conform to the acceptable use policy, will be reported through Impero and Fastview. This can then be actioned by a member of staff and recorded for evidence (Appendix E).
- The school has enhanced/differentiated user-level filtering for staff and students.
- All users (Years 1-6) will be provided with a username by AdEpt, 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 AdEpt 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.

5. 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 2019) as well as guidance from the Department for Education (Safeguarding Children in a Digital World) and CEOP (Child Exploitation and Online Protection).

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.

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.

6. 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 'Tapestry' 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.

Email
E-mail is a quick and easy method of communication, ensuring beneficial and appropriate usage is an important part of online safety: • Our Microsoft Education learning platform provides all children with a school e-mail address and password. (At present the email function of the account is disabled, however we look to introduce this if we can resolve some safeguarding concerns).

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.

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 F).
- 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.

Mobile Phones
Many mobile phones have access to the Internet and picture and video messaging. They present opportunities for unrestricted access to the Internet and sharing of images. 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. • 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. *This policy has been updated in line with 'Guidance for Safer Working Practice, May 2019'.*

7. Cyber Bullying

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

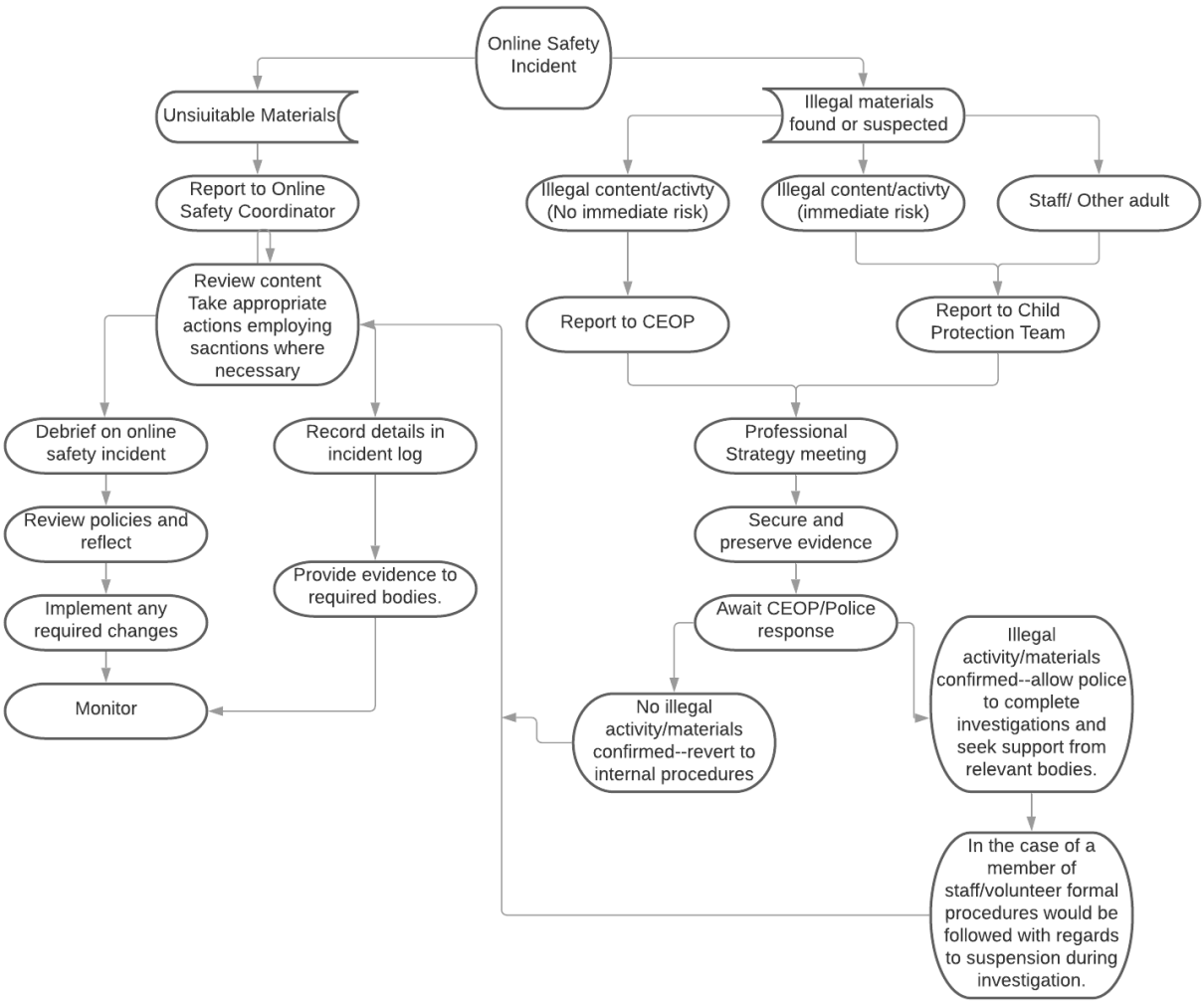
Bullying On-line and Social Media.

- 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.

APPENDIX A- Responding to issues of misuse



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

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.

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.

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 E- Safeguarding Running Log Recording Form

Date	Name
Alert	**Screen Shot (if Impero)**
Comments	

Actions	Actioned
•	
•	
•	
•	

APPENDIX F- Facebook Page Staff Guidelines

Beeston Primary School Facebook Page Staff Guidelines

- *Staff should only post photos of children who have provided a signed 'Photo Permission' form.*
- *When photographing or videoing children for Facebook posts, children without photo permission should be identified using a printed sticker. These children can then 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 names of children.*
- *Staff should not identify their location whilst on school trips or off-site therefore 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:* _____

When we use Teams for our Remote learning, we agree to:

- Only use the chat function to ask the teacher a question.
- Only use kind language when using the chat feature.
- Only upload pictures of work
- Not use the video feature, unless my teacher tells me to.
- If my teacher asks me to use the video feature, I will wear suitable clothes and have an adult sat with me.