

Beecroft Primary School Online Safety (E-safety) Policy – Revised August 2026

Contents of e-Safety Policy:

- 1. Introduction**
- 2. Context and background**
- 3. Roles and Responsibilities**
- 4. Technical and Hardware Guidance**
- 4 a. Filtering**
- 5. Online/e-Safety for pupils**
 - a. Internet access at school**
 - b. Using the Internet for learning**
 - c. Teaching the safe use of the Internet**
 - d. Using email with pupils**
 - e. Chat and online discussions**
 - f. Other online technologies – mobile phones etc**
 - g. Cyber Bullying**
 - h. PREVENT**
 - i. Creating of /SHARING images/video**
 - j. DATA PROTECTION (GDPR)**
 - k. Deliberate misuse – procedures and sanctions**
 - l. Complaints**
 - m. Remote Learning**
 - n. Artificial Intelligence**
- 6. Use of ICT by school staff: Staff Acceptable Use Agreement form**
- 7. Staff Social Media Policy – Agreement**
- 8. Pupils Acceptable Use Agreements (KS2/KS1/FOUNDATION)**

1. Introduction

Online safety is an integral part of safeguarding and requires a whole school, cross-curricular approach and collaboration between key school leads. Accordingly, this policy is written in line with 'Keeping Children Safe in Education' 2026 (KCSIE), 'Teaching Online Safety in Schools', statutory RSHE guidance and other statutory documents. It is cross-curricular (with relevance beyond Relationships, Health and Sex Education, Citizenship and Computing) and designed to sit alongside our school's statutory Child Protection & Safeguarding Policy. Any issues and concerns with online safety must always follow the school's safeguarding and child protection procedures. It is written in conjunction with the Beecroft's Anti-Bullying and Child Protection Policies and takes into account the Prevent Duty.

It has been discussed with staff, agreed by the senior management and approved by Governors. It will be reviewed annually.

At Beecroft we are passionate about the teaching of Online safety; it is an integral part of our preventative curriculum; it is taught throughout the year as a focus of every computing lesson. Every lesson starts with a reminder of the schools "SMART with a Heart" rules that children learn to BSL.

In addition to this each half-term, we have mapped out the 8 different strands of online safety from (Education For A Connected World). These objectives are taught both in and alongside children's normal computing lessons, in PSHE, using up to date resources from National Online Safety Center.

We realise it is the duty of the school to ensure that every child in our care is safe, and the same principles should apply to safeguarding them in the 'virtual' or 'digital' world, as would be applied to the school's physical buildings. We want to ensure that all of our Beecroft pupils create their own positive digital footprint.

This Policy document is drawn up to protect all parties: the students, the staff and the school and aims to provide clear advice and guidance on how to minimise risks and how to deal with any infringements.

Revised by:

S Campbell (ICT Co-ordinator)

Last Revised: August 2025

To be revised: August 2026

2. Context and Background

The technologies

ICT in the 21st Century has an all-encompassing role within the lives of children and adults, meaning issues around online safety are considerable and ever evolving. New internet and online technologies are enhancing communication and the sharing of information. Current and emerging Internet and online technologies used in school and, more importantly in many cases, used outside of school by children include:

- The Internet – World Wide Web
- Smart phones and Smart watches- with unlimited/unsupervised internet access
- Sharing and uploading of images from mobile devices
- GAMES consoles e.g. Xbox/Ps4 with online access
- Tablets/ laptops
- e-mail
- Instant messaging (including video chat and voice notes) e.g. Whatsapp
- Web based voice and video calling (e.g. Zoom/ Facetime)
- Online chat rooms
- Online discussion forums
- Social networking sites (e.g. Facebook/ Instagram)
- Other Social Media (Snapchat/ Tiktok)
- Blogs and Micro-blogs (e.g. Twitter)
- Podcasting (radio / audio broadcasts downloaded to computer or MP3/4 player)
- Video broadcasting sites/apps (e.g. You Tube/Tiktok)
- Music and video downloading (e.g. iTunes)

Our Whole School Approach To The Safe Use of ICT

Creating a safe ICT learning environment includes three main elements at this school:

- An effective range of technological tools;
 - Policies and procedures, with clear roles and responsibilities
 - Online-Safety teaching is embedded into the school curriculum and schemes of work
- Beecroft Primary School (Page 5)

3. Roles and Responsibilities

Online Safety is recognised as an essential aspect of strategic leadership in this school and the Head, with the support of Governors, aims to embed safe practices into the culture of the school.

Leadership team

The SLT ensures that the Policy is implemented across the school via the usual school monitoring procedures

Online-Safety Co-ordinator/ Online Safety Group

Our school online-Safety Co-ordinator is Steven Campbell (Deputy Headteacher). He leads the school Online Safety Group, which includes Nicola Brown (DSL), Rachel Pinder(PSHE), Emma Halliday(Y1 Computing teacher) and Qari Qasim (Parent Governor).

The group is responsible for keeping up to date on all Online-Safety issues and ensuring that staff are updated as necessary, making them aware of the potential issues that may arise from The 4 Cs (Keeping Children Safe In Education 2026):

content: being exposed to illegal, inappropriate, or harmful content, for example: pornography, racism, misogyny, self-harm, suicide, antisemitism, radicalisation, extremism, extreme sexual or physical violence, misinformation, disinformation (including fake news) and conspiracy theories,

contact: being subjected to harmful online interaction with other users or generative AI applications that simulate this; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes,

conduct: online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images, including those generated using AI (deepfakes) and online bullying, and

commerce: risks such as online gambling, inappropriate advertising, phishing and or financial scams. If you feel your pupils, students or staff are at risk, please report it to the Anti-Phishing Working Group (<https://apwg.org/>).

Governors

The School Governing body is responsible for overseeing and reviewing all school policies, including the e-Safety Policy. As mentioned above Mr Qasim is now part of the school online safety group.

School Staff

All teachers are responsible for promoting and supporting safe behaviours in their classrooms and following school e-Safety procedures. Central to this is fostering a 'No Blame' culture so pupils feel able to report any bullying, abuse or inappropriate materials.

- **Training with staff will be ongoing throughout the years' INSET programme.**
- **All staff will complete Online Safety/ Acceptable Use and Social Network training as part of their induction.**
- **All staff will complete the National Online Safety Certificate in Teaching Online Safety Annually in July or on induction starting work at the school.**

All Beecroft staff are responsible for ensuring that:

- they have an up to date awareness of e-safety matters and of the current school e-safety policy and practices

- they have read, understood and signed the school Staff Acceptable Use Policy (AUP)
- they report any suspected misuse or problem including Child on Child Abuse to the Designated Lead for Safeguarding and E-Safety for investigation, action or sanction
- digital communications with pupils should be on a professional level and only carried out using official school systems
- e-safety issues are embedded in all aspects of the curriculum and other school activities
- pupils understand and follow the school e-safety and acceptable use policy
- pupils have a good understanding of research skills and uphold copyright regulations
- they monitor ICT activity in lessons, extra curricular and extended school activities
- they are aware of e-safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices
- In lessons where internet use is pre-planned pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches
 - Teacher will vet any videos to be used to aid teaching beforehand, especially Youtube where ads and pop ups are present.
 - Class teachers should ensure that pupils are aware of SMART (with a heart) rules, introducing them at the beginning of each new school year; then embedding them with regular weekly discussion.

Pupils

Pupils are expected to take an active part in planned lessons and activities to support their understanding and confidence in dealing with e-Safety issues, both at home and school.

They are asked to agree to a set of guidelines and rules covering their responsibilities when using ICT at school

Parents

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet and mobile devices in an appropriate way. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of ICT than their children. The school will therefore take every opportunity to help parents understand these issues through family assemblies, newsletters, letters and information about national and local e-safety campaigns and literature. Parents and carers will be responsible for endorsing the Pupil Acceptable Use Policy.

(Page 6)

Technical Support

The ICT Service Provider is currently SchoolsICT (Formerly Connect-up). Our managed service technician is Billy Loxton, who visits school on Wednesdays for a full day to maintain our hardware, software and computing, infrastructure.

They are responsible for ensuring:

- that the school's ICT infrastructure is secure and is not open to misuse or malicious attack
- that Beecroft meets the e-safety technical requirements outlined in the Acceptable Usage Policy and any relevant DFE or Local Authority E-Safety Policy and guidance
- that users may only access the school's networks through a properly enforced password protection policy, in which passwords are regularly changed
- the school's filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person.
 - That the school's filtering system meets DFE requirements and is reviewed annually
- That it keeps up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant.

4. Technical and hardware guidance

School Internet provision

The school uses the standard LA Internet Service Provider, which is Talkstraight driven *Schoolsbroadband, who we have reviewed to be the best new provider with filtering meeting DFE requirements.*

Talkstraight provides an always-on broadband connection at speeds up to 50mb and:

☑ E-safety, secure filtered access to the internet via 'Smoothwall' Technology and Man in the Middle security

☑ E-mail using Leeds enterprise partner Microsoft- Anti- Virus provided by (Sophos)

4a. Content filtering

Schoolsbroadband use a sophisticated netseeper *Smoothwall* content filter to ensure that as far as possible, only appropriate content from the Internet finds its way into school.

As stated in the DFE guidance (March 2023) *No filtering system can be 100% effective. You need to understand the coverage of your filtering system, any limitations it has, and mitigate accordingly to minimise harm and meet your statutory requirements in [Keeping children safe in education](#) (KCSIE) and the [Prevent duty](#).*

Our provider Talkstraight Schoolsbroadband is:

- a member of Internet Watch Foundation (IWF)
- signed up to Counter-Terrorism Internet Referral Unit list (CTIRU)

- blocking access to illegal content including child sexual abuse material (CSAM)

The filtering system is updated weekly and applied to all:

- users, including guest accounts (pupil and staff have different age specific levels of access)
- school owned devices (Includes all laptops/ ipads and school chromebooks)
- devices using the school broadband connection - all devices must be added to the network first by the ICT technician using “man in the middle” technology – this prevents any unauthorised access of the internet for staff/ pupils alike

Our school filtering system:

- filters all internet feeds, including any backup connections
- Is age and ability appropriate for the users in our educational setting
- handles multilingual web content, images, common misspellings and abbreviations
- identifies technologies and techniques that allow users to get around the filtering such as VPNs and proxy services and block them
- provide alerts when any web content has been blocked - These alerts are sent instantly to Mr Campbell’s email so that he can tackle any incidents/ breaches and rectify any issues.
- Talkstraight Schools broadband provides the same filtering on all of our school’s mobile or app technologies including ipads and VR headsets.
- If the case arises individuals who might be trying to access unsuitable or illegal material so they can be supported by appropriate staff, such as the senior leadership team or the designated safeguarding lead.

The filtering breach alerts notify the Deputy of:

- device name or ID, IP address, and where possible, the individual
- the time and date of attempted access
- the search term or content being blocked

This allows any further action to be taken easily.

- All pupils and staff have been issued with clear guidelines on what to do if this happens, and parent will be informed where necessary.

- Pupils or staff who deliberately try and access unsuitable materials will be dealt with according to the rules outlined elsewhere in this document.

- SC has a log of all filtering breaches and actions taken. He liaises with NB (DSL) as to whether any further safeguarding actions are needed.

This filtering is reviewed annually (July) by S Campbell, Billy Loxton and Talkstraight Schools broadband using Smoothwall.

Downloading files and applications

The Internet is a rich source of free files, applications, software, games and other material that can be downloaded and installed on a computer. Whilst some of this material may be useful, much is inappropriate, and may adversely affect the performance and reliability of school equipment.

- Pupils are not allowed to download any material from the Internet unless directed to do so by an appropriate staff member. (note: Downloaded content can only be run/opened by an administrator which is password protected)

Portable storage media

- Staff are allowed to use their own portable media storage if it is encrypted (USB Keys etc) but no sensitive data should be taken from the premises. Sensitive data must be stored on encrypted storage devices (GDPR).

If use of such a device results in an anti-virus message they should remove the device and immediately report to the ICT Administrator. (All items are automatically scanned by SOPHOS) in-line with GDPR unless they are encrypted.

- Where possible teachers should use their School Office 365 Onedrive for storage, which is secure.

Security and virus protection

The school subscribes to the LA Antivirus software program, which uses Sophos Antivirus software. The software is monitored and updated regularly by the school technical support staff

- Key words are regularly checked inline with PREVENT and CTRIU filter list.
- Any software messages or pop-up screens reporting evidence of viral infection should always be reported immediately to the ICT Administrator

5. e-Safety for Pupils

We believe it is our responsibility to prepare pupils for their lives in the modern world, and ICT is an integral part of that world. At our school we are committed to teaching pupils to use the ICT effectively and appropriately in all aspects of their education.

a) Internet access at school

Use of the Internet by pupils

Internet access is carefully controlled by teachers according to the age and experience of the pupils, and the learning objectives being addressed. Pupils are always actively supervised by an adult when using the Internet, on laptops and ipads.

Access for all pupils

In line with our inclusion policies across the school, we want to ensure that all our pupils have access to the Internet, particularly where this will directly support their learning.

Out of Hours Provision

To this end, we provide morning access and support for pupils at drop in sessions from 8.30-8.45am, where children can use TTRockstars or IXL maths.

b) Using the Internet for learning

The Internet is now an invaluable resource for learning for all our pupils, and we use it across the curriculum both for researching information and a source of digital learning materials.

Using the Internet for learning is a vital part of the curriculum, so we teach all of our pupils how to find appropriate information on the Internet, and how to ensure as far as possible that they understand who has made this information available, and evaluate how accurate and truthful it is.

- Teachers carefully plan all Internet-based teaching to ensure that pupils are focussed and using appropriate and relevant materials.
- Children are taught how to use search engines and how to evaluate Internet-based information as part of the Computing curriculum, and in other curriculum areas where necessary.
- They are taught how to recognise the difference between commercial and non-commercial web sites, and how to investigate the possible authors of web-based materials.
- They are taught how to carry out simple checks for bias and misinformation (RELIABILITY)
- They are taught that web-based resources have similar copyright status as printed and recorded materials such as books, films and music, and that this must be taken into consideration when using them. Beecroft Primary School Page 8 e-Safety Policy

c) Teaching safe use of the Internet and ICT

We think it is crucial to teach pupils how to use the Internet safely, both at school and at home, and we use the Kidsmart safety code to support our teaching in this area: Kidsmart has been developed by the Childnet charity, and is endorsed by the DfES

<http://www.kidsmart.org.uk>

The main aspects of this approach include the following five SMART with a heart tips:

Safe - Staying safe involves being careful and not giving out your name, address, mobile phone no., school name or password to people online...

Meeting someone you meet in cyberspace can be dangerous. Only ever do so with your parents'/carers' permission and then when they are present...

Accepting e-mails or opening files from people you don't really know or trust can get you into trouble - they may contain viruses or nasty messages...

Respect - Treat people online with respect no matter whether you are chatting on a game, sending a message or commenting on a video. Always be kind. Think: would I like this said to me? Would my mum or dad be happy hearing what I am saying? OR IN KS2 M-

Reliable someone online may be lying and not be who they say they are. If you feel uncomfortable when chatting or messaging end the conversation. Not everything you read online is true <https://www.factcheck.org/>

Tell your parent or carer if someone or something makes you feel uncomfortable or worried...

...**with a heart**always be kind and respectful online, treating people the way in which you wish to be treated yourself.

Make sure your digital footprint is a positive one.

Suitable material:

We encourage pupils to see the Internet as a rich and challenging resource, but we also recognise that it can be difficult to navigate and find useful and appropriate material. Where possible, and particularly with younger children, we provide pupils with suggestions for suitable sites across the curriculum, and staff always check the suitability of websites before suggesting them to children, or using them in teaching.

Any Youtube videos must be vetted beforehand for age-appropriateness (checking ads, comments, and content), turning off autoplay. Teachers must have watched the full video prior to the lesson; avoiding searching in front of students. Teachers should load the video in school, on their laptop first, without the Clevertouch screen attached to ensure it loads the same as it did they planned/vetted it.

Non-Education materials:

We believe it is better to support children in finding their way around the Internet with guidance and positive role modelling rather than restrict Internet use to strict curriculum based research.

As well as Internet material directly related to the curriculum, we encourage children to visit appropriate entertainment and child-oriented activity sites that have interesting and relevant activities, games and information, in free time at out-of-school-hours provision, and at home.

There is a selection of links to such resources available from on the school website, and in the shared pupil folders on the school network.

Unsuitable material:

Despite the best efforts of the LA and school staff, occasionally pupils may come across something on the Internet that they find offensive, unpleasant or distressing. Pupils are taught to always report such experiences directly to an adult at the time they occur, so that action can be taken.

The action will include:

1. Making a note of the website and any other websites linked to it.
2. Informing the ICT Administrator
3. Logging the incident (S Campbell) Cpoms
4. Discussion with the pupil about the incident, and how to avoid similar experiences in future

Beecroft Primary School Page 9 e-Safety Policy

d) Using E-Mail at school

E-Mail is a valuable and stimulating method of communication that plays an important role in many aspects of our lives today. We believe it is important that our pupils understand the role of e-mail, and how to use it appropriately and effectively.

- We teach the use of e-mail as part of our ICT curriculum, and use appropriate pupil email accounts where necessary (Year 6 for home-school learning on their chromebooks will use their school office 365 pupil accounts e.g. Joe.bloggs@stu.beecroft.leeds.sch.uk)
- Pupils are not allowed to access personal e-mail using school Internet facilities
 - As much software we use is now online based e.g. Appshed or Google Sketchup, the school has created generic Gmail accounts which are assigned to pupils when needed and monitored. These passwords cannot be changed by children.

e) Chat, discussion and social networking sites

These forms of electronic communication are used more and more by pupils out of school, and can also contribute to learning across a range of curriculum areas. Online chat rooms, discussion forums and social networking sites present a range of personal safety and privacy issues for young people, and there have been some serious cases highlighted in the media.

We use the resources, guidelines and materials offered by Kidsmart, as outlined above in the Safe use of the Internet section to teach children how to use chat rooms safely.

Weekly guides from National Online Safety are sent out to parents(WakeUP Wednesday) in order to inform them about new and evolving dangers/ risks/.

All commercial Instant Messaging and Social Networking sites are filtered/banned as part of the LA in our children's access accounts; all staff have signed an agreement not to use these in school.

Internet policy

Pupils may take part in discussion forums or post messages on bulletin boards that teachers have evaluated as part of specific lesson activities. Individual pupil names or identifying information will never be used.

f) Smart phones/ Smart Watches and handheld devices

More and more young people have access to sophisticated new internet-enabled devices such as SMART mobile phones, watches tablets, games consoles and music players.

It is important that whilst the school recognises the potential advantages these devices can offer, there are clear and enforceable rules for their use in school, particularly when they give access to the Internet, and allow pictures and information to be remotely posted to a website or weblog.

Pupils will be taught the legal and moral implications of posting photos and personal information from mobile phones to public websites etc and how the data protection and privacy laws apply.

- Pupils are not allowed to have personal mobile phones or other similar devices in school e.g. smart watches (This is the same for staff who must keep them in lockers/ bags to be used away from children in break times only). Parents may request that such devices are kept at the School Office for pupils who may need them on their journey to and from school.

- Children in both Key Stages are taught about 'consent' to having their photo taken; we emphasise the need to be 'share-aware'.
- In Y5/6 children are taught about the growing threat of 'sexting' using the NSPCC's 'I saw your willy' video. The emphasis is on never to take or allow to be taken, indecent images of themselves. We ensure they understand the implications if these were to be shared around or become viral.

g) Cyberbullying - Online bullying and harassment

Online bullying and harassment via Instant messaging, mobile phone texting, e-mail and chat rooms are potential problems that can have a serious effect on pupils. Our school has a range of strategies and policies to prevent online bullying, outlined in various sections of this policy.

These include:

- No access to public chat-rooms, Instant Messaging services and bulletin boards.

- Pupils are taught how to use the Internet safely and responsibly, and are given access to guidance and support resources from a variety of sources.
 - We encourage pupils to discuss any concerns or worries they have about online bullying and harassment with staff, and have a range of materials available to support.
 - This links in conjunction with the schools' TELL poster and policy; encouraging children to discuss any worries or fears they may have.
- Complaints of cyber-bullying are dealt with in accordance with our Anti-Bullying Policy.
- Complaints related to child protection are dealt with in accordance with school child protection procedures.
- Staff are trained to report any concerns of child on child abuse including sending of nasty messages on Whatsapp or sharing of nudes/semi nudes.

h) Prevent

Section 26 of the Counter-Terrorism and Security Act 2015 (the Act) places a duty on certain bodies ("specified authorities" listed in Schedule 6 to the Act), in the exercise of their functions, to have "due regard to the need to prevent people from being drawn into terrorism".

There are a range of offences in relation to incitement of hatred on the basis of race, religion, sexual orientation and particular offences concerning harassing or threatening individuals which includes cyber bullying by mobile phone and social networking sites etc. It is an offence to send indecent, offensive or threatening messages with the purpose of causing the recipient distress or anxiety. Pupils are taught about tolerance through day to day discussion, trips, visits and literature. Whilst in Key Stage 2 children learn about the consequences of posting hateful material online, understanding that there may be extremist views online that are trying to influence them and how to stay safe from this.

Staff are trained that if they come across any articles, images, speeches or videos that promote terrorism or encourage violence including content encouraging people to commit acts of terrorism, websites made by terrorist or extremist organisations or videos of terrorist attacks they can report this at <https://www.gov.uk/report-terrorism>.

They must report to SLT if they suspect any links to radicalisation. We use the CTRIU filter list tool to ensure that there is no access to any such websites or materials in school.

i) Creating Images of Students through Video or Photography

Many work based activities involve recording images and these may be undertaken as part of the curriculum, extra school activities, for publicity, or to celebrate achievement.

However, written permission must be gained from legal guardians prior to creating images of students. Parents sign a photo consent form held in the school office.

Using images of students for publicity purposes requires the age appropriate consent of the individual concerned and their legal guardians. Images should not be displayed on websites(e.g. our private Youtube account), 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.

Photograph or video images must be created using equipment provided by the work place ie. School ipads. It is not acceptable to record images of students on personal equipment such as personal cameras, mobile phones or video camera. Images of students must not be created or stored for personal use.

Members of staff creating or storing images of students using personal equipment without prior consent will be subject to disciplinary action.

Members of staff must:

- be clear about the purpose of the activity and about what will happen to the photographs when the lesson/activity is concluded (;
- ensure that senior management is aware that photography/image equipment is being used and for what purpose;
- ensure that all images are available for scrutiny in order to screen for acceptability;
- be able to justify images of students in their possession;
- avoid making images in one to one situations.

Members of staff must not take, display or distribute images of students unless they have consent to do so. Failure to follow any part of this code of practice may result in disciplinary action being taken.

For further guidance on creating, displaying and storing images of students please refer to the Safer Working Practice Guidance (HR Schools 2014) as well as guidance from the Department for Education (Safeguarding Children in a Digital Work) and CEOP (Child Exploitation and Online Protection)

j) Contact details and privacy (GDPR)

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights

- Secure
- Only transferred to others with adequate protection.

Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
 - Use windows +L Key to lock their laptops if going away from the machine for extended period of time.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly “logged-off” at the end of any session in which they are using personal data.
- Transfer data using encryption and secure password protected devices or the School OFFICE 365 onedrive.

When personal data is stored on any portable computer system:

- the data must be encrypted and password protected
- the device must be password protected
- the device must offer approved virus and checking software
- the data must be securely deleted from the device, in line with school policy once it has been transferred or its use is complete

Pupils are taught that sharing this information with others can be dangerous – see Teaching the Safe Use of the Internet.

- School and pupil websites – pictures and pupil input
- As part of the ICT and wider curriculum, pupils may be involved in evaluating and designing web pages and web-based resources.
- Any work that is published on a public website and attributed to members of our school community will reflect our school, and will therefore be carefully checked for mistakes, inaccuracies and inappropriate content.
- Pupils may design and create personal web pages. These pages will generally only be made available to other school users, or as part of a password protected network.
- Where pupil websites are published on the wider Internet, perhaps as part of a project with another school, organisation etc, then identifying information will be removed, and images restricted.

k) Deliberate misuse of the Internet facilities

All pupils have discussed the rules for using the Internet safely and appropriately and signed their pupil agreement (annually in September).

Where a pupil is found to be using the Internet inappropriately, for example to download games, or search for unsuitable images, then sanctions will be applied according to the nature of the misuse, and any previous misuse.

Sanctions will include:

For viewing Unsuitable material (e.g. online games, celebrity pictures, music downloads, sport websites etc)

- Initial warning from class teacher
- Banning from out of school hours Internet facilities
- Report to Headteacher
- Letter to parent/carer
- Offensive material (e.g. pornographic images, racist, sexist or hate website or images etc) Incident logged and reported to Head teacher
- Removal of Internet privileges/username etc

I) How will complaints regarding e-Safety be handled?

It is the duty of the school to ensure that every child in our care is safe, and the same principles should apply to the 'virtual' or 'digital' world as would be applied to the school's physical buildings. international scale and linked nature of Internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device. Neither the school nor the Local Authority can accept liability for material accessed, or any consequences of Internet access.

Staff and pupils are given information about infringements in use and possible sanctions.

Sanctions available include:

- All incidents will be recorded (CPOMs)
- Interview/counselling by class teacher, Senior Management Team, e-Safety Coordinator and Headteacher;
- informing parents or carers;
- removal of Internet or computer access for a period,
- referral to LADDO / Police if serious

Our e-Safety Coordinator acts as first point of contact for any complaint. Any complaint about staff misuse is referred to the Head teacher.

M. Remote Learning

(Please see Remote Learning Policy for staff/pupil/parent agreements and details)

- Any remote learning will be carried out through the school's chosen digital platform Microsoft Teams, which is secure.
- Children and staff have been trained how to use it safely.
- Children are able to borrow one of the 80 school chromebooks/ or 64 curriculum laptops if both parent and pupil have signed the acceptable use agreement.
- The home use school chromebooks have been locked down to safe search using the same filtering that pupils use in school. This has been 'key word' tested by Connect-up and shown to only include educational results.
- Websites that could be accessed such as Youtube have been set to child mode so that there is no inappropriate material.
- Children cannot download their own apps or adjust laptop settings.
- Laptops have had a home learning profile created with only Teams/Office and Chrome available. It will be parents' responsibility to monitor home internet use.
- Children/parents have signed an agreement to ensure they are fully clothed not in pyjamas for all online sessions. There are no lessons to be done in bedrooms by either staff or pupils.
- Staff will ensure when screen sharing there is only the required educational material on show and nothing personal including photo backgrounds.
- Teachers will record their lessons so that they could be reviewed at a later date and keep a register of children who attend the online sessions.
- All chromebooks have a tracking app enabled.
- All staff will follow safeguarding procedures and will report any cause for concerns that arise from their remote learning in the usual way in school to DSL (N Brown) and SLT.
- If pupils or parents misuse TEAMS or school devices, they will receive a call from the headteacher. A decision will then be made whether or not to remove pupil access to TEAMS or device and invite the pupil back into school for their learning.

N- Artificial Intelligence

Please see separate Artificial Intelligence Policy

All teachers watch and understood the DFE video

<https://www.youtube.com/watch?v=Hs6gmNoMhqM> Protecting children's privacy when using Artificial Intelligence, before they use any AI tools in school. This is part of their September annual Safeguarding training and is part of the teachers' safe IT use agreement (from September 2026).

Staff are trained in the dangers AI presents for children particularly the growing trend of web scraping for images which can be used in deep fakes creating child abuse material. They know the need to safeguard children against this and how to safely report an instance.

Staff know that although they may use AI to help them in the cutting down their work load to aid with planning and resources; all AI generated materials must however be vetted before use with children as it may be:

- inaccurate

- inappropriate or unsafe
- biased
- taken out of context
- taken without permission (intellectual property infringement)
- out of date or unreliable
- low quality

No AI can be used 'live' as part of a lesson because of this.

- **Any AI tools used in school must be agreed and approved by governors. Our main tool which is approved for its safety features is Microsoft Copilot.**
- **In line with GDPR training staff know they are never to put pupil data, pupil images/ personal information into AI tools.**

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

- seek advice from our data protection officer or IT lead
- check that the type of tool being used is approved by our school
- understand how the tool uses personal data and whether this adheres to your school's data protection policy
- acknowledge or reference the use of generative AI in your work
- fact-check results to make sure the information is accurate

6. Beecroft Staff Acceptable ICT Use Agreement

Beecroft Staff Acceptable Use Policy Agreement for ICT 2026/2027

I understand that I must use Beecroft Primary School ICT systems in a responsible way, to ensure that I safeguard both myself and pupils, comply with GDPR regulations and cyber-security. I recognise the value of the use of ICT for enhancing learning and will ensure that all pupils receive opportunities to gain from the use of ICT. I will at all times educate pupils in my care about the safe and responsible use of ICT, following the SMART rules and creating a positive digital footprint .

For my professional and personal safety:

- I understand that the school will monitor my use of the ICT systems, email and other digital communications. A daily report is sent to S Campbell (Computing Lead) of all pupil and staff's internet searches.
- I understand that the rules set out in this agreement also apply to use of school ICT systems (e.g. laptops, email, ipads etc) out of school.
- I understand that the school ICT systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password.
 - I will use 2 FA Microsoft Authenticator to log into schools' Office 365 email system. I will report any problems with to this system to SC and B. Loxton (school IT Technician) immediately.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the IT lead SC.
 - I will be professional in my communications and actions when using school ICT systems.
- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
 - To comply with GDPR I will use windows +L function to lock my laptop/ PC if leaving it unattended for an extended period of time.

- I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital / video images.
 - **I will never use my personal equipment to take photographs, images or recordings of pupils.** Where these images are published (e.g. on the school website) it will not be possible to identify by name, or other personal information, those who are featured. All pupils must have parental consent for this (see photographs in school policy)
- I will not use social media in school, unless in private areas like the staffroom (away from pupils), in my own time, in accordance with the school's policies.
- I will only communicate with students / pupils and parents / carers using official school systems (e.g. Parentmail). Any such communication will be professional in tone and manner.
- I will not engage in any on-line activity that may compromise my professional responsibilities.

Beecroft Primary and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- When I use my personal hand held / external devices (laptops / mobile phones / USB devices etc) in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by the school about such use (see below). I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.

Staff Mobile Phones/SMART watches:

- Staff/Volunteers/ Peripatetic teachers/Visitors are not permitted to make/receive calls/texts during contact time with children. Emergency contact should be made via the school office.
- Staff should have their phones on silent or switched off and out of sight (e.g. in locker/ a drawer or cupboard) during class time.
 - Smart watches may be worn by staff, but as per the school social media agreement must have notifications switched off and not be used to access the web in teaching time.
 - Staff must not use their personal smartwatch to process personal data, or any other confidential school information.
 - Meta glasses or similar smart glasses are strictly forbidden.
- Mobile phones should not be used in a space where children are present (e.g. classroom, playground).

- Use of phones (including receiving/sending texts and emails on smart watches and mobile phones) should be limited to non-contact/break time when no children are present e.g. in office areas, staff room, empty classrooms.
- It is also advised that staff security protect access to functions of their phones.
- Should there be exceptional circumstances (e.g. acutely sick relative), then staff should make the Head teacher aware of this and arrangements will be made with the school office so that the emergency call can be received.
- Staff are not at any time permitted to use recording equipment on their mobile phones/smart watches, for example: to take recordings of children, or sharing images. Legitimate recordings and photographs should be captured using school equipment such as cameras and ipads (these must be stored on the teacher share system as per the photos in school policy)
- Staff should report any usage of mobile devices that causes them concern to teacher
 - Mobile/Smart phones are permitted to be used on school trips/residential to keep in contact with school, but again must follow the above rules.
 - The after school club phone will be made available for sports events/ off site activities where direct contact with parents may be required. This must be appropriate and professional. Where possible though, parent contact should be made through the school office/ parentmail.

Other school systems:

- I will not use personal email addresses on the school ICT systems.
- I will not open any attachments to emails, unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programs.
 - If this happens I must notify S Campbell immediately as per the GDPR policy, to assess if there has been a phishing attack.
- I will ensure that my data is regularly backed up (One Drive), in accordance with relevant school policies.
 - I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or anything inappropriate that may cause harm or distress to others.
 - I will not try to use any programs or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will not install or attempt to install programs of any type on a machine, or store programs on a computer, nor will I try to alter computer settings, unless this is allowed in school policies. Consult SC and B.Loxton to do this on your behalf.

- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School Data Policy (GDPR).
 - **In line with the GDPR policy I will use my school Onedrive to save/transfer files between school/home. I will only use a USB drive if it is encrypted.**
 - I understand that data protection policy requires that any staff or pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary, or that I am required by law or by school policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the internet in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).
 - In lessons where internet use is pre-planned pupils I will ensure pupils are guided to sites I have checked as suitable for their use
 - I will vet any videos to be used to aid teaching beforehand, especially Youtube where ads and pop ups are present.
 - I will never search for a video on Youtube ad-hoc in front of the children. Videos must be pre-loaded before the lesson/ before the laptop screen is shared to the Clevertouch screen.
 - I will report any issues that arise with filtering to the IT Lead SC.

Artificial Intelligence

- I have watched and understand: <https://www.youtube.com/watch?v=Hs6gmNoMhqM> Protecting children's privacy when using Artificial Intelligence, before they use any AI tools in school.
- I have read and will follow the school's Artificial Intelligence Policy.
- I will not use any Artificial Intelligence tool/software or assistant, unless it has been governor approved and meets generative-ai-product-safety-standards.
- I understand that Microsoft Copilot is the only approved safe AI tool to use in school for my own work.
- In Year 6 pupils will be taught about AI but are not yet permitted to use it themselves in school.
- I can use AI at home (e.g. Chat GPT) to help with my planning and resources but will never use it with personal data about school or pupils.

- I will not ask AI to produce a result in front of children whether it be in the form of text/ voice/ picture or video as this could expose them to inappropriate or harmful material.
- Any AI produced resources I use must be vetted before use by pupils.

I understand that I am responsible for my actions in and out of school:

- I understand that this Acceptable Use Policy applies not only to my work and use of school ICT equipment in school, but also applies to my use of school ICT systems and equipment out of school and my use of personal equipment in school or in situations related to my employment by the school.
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors and / or the Local Authority and in the event of illegal activities the involvement of the police.

I have read and understand the above and agree to use the school ICT systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Staff / Volunteer Name

Signed

Date

7. Staff Social Media Use Agreement Beecroft

Beecroft Staff Online Safety Policy : Use Of Social Media Platforms

Agreement 2026/27

At Beecroft Primary school, we acknowledge that social media platforms (e.g. Facebook/Instagram/Snapchat and Tiktok) can provide a valuable learning resource and are a way of keeping in touch with friends and family. However, the nature of teaching and working in education means that school staff must be particularly aware of their online reputation (Safer Working Practise) to safeguard both themselves and pupils.

KCSIE 2026 states that, *"As part of the shortlisting process, schools and colleges should consider carrying out a search (via an online search engine) as part of their due diligence on the shortlisted candidates."*

This safer recruitment search is designed to identify:

- Content that suggests a risk to child safety, including inappropriate interactions with minors, extremist views, or content that normalises harmful behaviour
- Evidence of serious professional misconduct that is not reflected in the DBS record
- Discriminatory, racist, or abusive content that conflicts with a school's values and equalities duties
- Behaviour that demonstrates a pattern of poor professional judgement
- Content that contradicts information provided in the application or interview

The DFE's Online Safety Guidance for staff (July 2026) states online safety is an important part of your professional conduct and personal security.

This agreement is to help you:

- meet expected standards of online behaviour
- protect your personal and school-wide digital security
- safeguard your online reputation
- reduce the risk of online bullying or harassment

To protect myself as a staff member of Beecroft Primary School I agree to:

- **Never accept friend requests on my personal accounts or accept requests to follow me from pupils, past pupils or even parents at our school.**

- I will report this to senior leaders if I receive such a request.
- I will ensure I understand the privacy and security settings of any social media and apps I use and keep them up to date.
- I will regularly check on my online presence (for example, by typing my name into a search engine) so that any negative content can be dealt with as soon as it appears.
<https://saferinternet.org.uk/guide-and-resource/teachers-and-school-staff/professional-reputation>
- I will not make personal social media posts about the school, its staff, pupils, past pupils or parents in an online environment – even if my account is private. Posting derogatory comments about the school, employer, pupils, parents or colleagues **is never acceptable.**
- I am aware that my reputation could be harmed by what others share about me online (for example, if am tagged in inappropriate posts, photographs or videos). It is my responsibility to discuss this with family, friends and colleagues.
- I will think about the language I use – abrupt or inappropriate comments, even if they were made in jest, may lead to complaints. Anything that is put online is potentially public and permanent.
- I will choose a profile image carefully and be mindful about what ‘liking’ certain pages/ posts or groups says about my reputation.
- I understand I am required to uphold the reputation of the school, to maintain reasonable standards in my own behaviour, and to uphold public trust in the profession.
- I will use a strong passwords for my accounts, including: capitals, lower case, symbols and numbers. I should consider using biometrics and 2FA where possible.
- I am aware of the need to keep my personal information private to avoid identity theft/ fraud and scams including the growing trend of AI Social Media Scraping.
- I will consider making private, or removing, previous online content that might compromise my current position. It is possible to deactivate existing SNS accounts and to permanently delete profiles.
- I will not use school machines to access social media. It can only be accessed in my own time away from pupils sight (e.g. in staff room) on my own devices.
- If I wear a smart watch all social media notifications/alerts will be switched off in school.
- If I come across, or are made aware of, inappropriate use of social media sites by our pupils (including under age use of these services), you should report this safeguarding concern to myself(SC) or the Head (JT).

I have read the guidance for Safe Use of Social Media Platforms and agree to follow the policy.

Signed _____ Date _____

Print _____

8. Beecroft Primary School Class Rules for responsible ICT use

Keep safe: Keep SMART

1. I will ask permission before using any ICT equipment (e.g. Chromebooks, Laptops, Clevertouch, Ipads or VR headsets), and only use it when a teacher or another adult is with me.
2. I will not bring my mobile phone or smart watch to school. I will only use the school's computers for schoolwork and homework.
3. I will only delete my own files, and I will not look at other people's files without their permission.
4. I will use the usernames and passwords provided by the school to access the school network
5. I will not bring software or USB memory sticks into school without permission
6. I will ask permission before using the Internet, and only use it when a staff member is present. I know I am not to search using AI tools.
7. I will only visit web sites that I am asked to by school staff, or that have been saved in a shared internet link folder for pupils to use
8. I will not use Google image search without being asked to do so by a school staff member.
9. I will not download anything (files, images etc) from the Internet unless given permission
10. I will only use an approved email account provided for me by the school to send email as part of my learning. I will not use personal email accounts (e.g. Hotmail) at school. As part of curriculum from

time to time I will be allowed to use the school's own generic gmail accounts. These are for school use only.

11. The messages I send or information I upload as part of my school work will always be polite and respectful.

12. I will not give my home address, phone number, send a photograph or video, or give any other personal information online that could be used to identify me, my family or my friends, unless my teacher has given permission

13. If I see anything that makes me uncomfortable, or I receive a message I do not like, I will not respond to it but I will immediately tell a school staff member

14. I will follow the SMART rules at all times.

15. I understand that the school may check my computer files, e-mail and the Internet sites I visit, to help keep me safe.

16. I will not make any changes to laptop settings, ipad settings or apps without permission.

17. I understand that if I deliberately break these rules my parents and the Headteacher will be informed and I may have my internet or computer access withdrawn.

18. I agree to try and create my own digital footprint that is positive.

Signed _____ Class _____
DATE _____

Rules for acceptable use of ICT and the internet.

Reception and KS1

**Our ICT rules help us to enjoy using computers
and they keep us safe:**

- I will ask my teacher if I want to use the chromebook, laptop, clevertouch screen or ipad.
- I will not bring any devices of my own to school including smartphones, smart watches or tablets.
- I will only use programs or websites that my teacher has told me to use.
- I will only search for words my teacher has told me to.
- I will ask my teacher if I want to do something new or different on the computer
- I will take care of the laptop, ipad and other ICT equipment
- I will not click on keys or links, if I don't know what they do.
- I ask for help from an adult if I am not sure what to do or if I think I have done something wrong.
- I will always tell an adult if I see something unexpected or that upsets me on the screen.
- If I break the rules I will miss my turn on a computer/ipad/chromebook or laptop.
- I will always be kind and respectful when using laptops, ipads or going online.
- If I have seen something that upsets me when I go online at home I will tell my teacher.
- I will follow the SMART rules.

Signed (child):.....



Beecroft Foundation Stage
Our ICT Rules

Our ICT rules help us to enjoy using computers and they keep us safe.

- I can use the ipad, totem touch, laptop if I have planned to do so with my teacher.



- I will always be very careful using ipads, computers and ICT equipment.
- If I am not careful I will not be able to use the ipads/computers.
- I will tell an adult if something comes up on the screen that I do not understand, or upsets me.

Signed (child):.....

Signed (parent):

