Beardall Fields Primary and Nursery School
E-Safety Policy

Our e–Safety Policy has been written by the school, building on the Nottinghamshire LA and government guidance.

Our School Policy has been agreed by the Senior Leadership Team and approved by governors

The School has appointed a member of the Governing Body to take lead responsibility for e-Safety.

The School e-Safety Lead is Charlene Graham

The date for the next policy review is September 2025 or sooner in the event of an issue arising.

Teaching and Learning

Vision: Children are able to access and use technology safely, making sensible choices about their own and others wellbeing.

What do we mean by technology?
Technology within this policy means electronic equipment which provides us with information. Technology is another word for ICT (Information Communication Technology)
This includes the hardware, such as laptops, tablets and ipads and desktop computers and software which are the programmes and applications which people use. Examples of software programmes include Microsoft Office tools such as Word. This definition also includes the things which are harder to see, such as the internet and computer network. These are types of ICT services.

How does technology benefit education?
ICT benefits learning and teaching in the following ways:

- Provides an engaging and motivational way to learn.
- Allows pupils access to a rich variety of multimodal information eg. video, audio, images, text.
- Allows pupils to connect to learning in accessible ways eg. by providing a writing framework or having the computer read instructions to them.
- Supports high quality teaching through the use of diverse and interactive resources.
- Supports a collaborative approach to learning.
- Supports personalisation by providing flexibility in the pace, place and time of learning.
- Culturally enriching by connecting pupils to people and communities in different localities.

The internet can provide the following specific benefits:

- Access to worldwide educational resources.
- Educational and cultural exchanges between pupils worldwide.
- Access to experts in many fields for pupils and staff.
- Professional development for staff through access to national developments, educational materials and effective curriculum practice.
- Collaboration across networks of schools, support services and professional associations.
- Exchange of curriculum and administration data.
- Access to learning wherever and whenever convenient.

How can internet use enhance learning?

- Education can happen both at home and at school.
- Internet research, including the skills of knowledge location, retrieval and evaluation.
- Online activities that support the learning outcomes planned for the pupils' age and ability.
- Pupils learn to acknowledge the source of information used and to respect copyright when using Internet material in their own work.

Pupils will be taught what internet use is acceptable and what is not and given clear objectives for internet use. Copyright law will be adhered to by the school when using materials from the Internet.

How will pupils learn how to evaluate internet content?

- Critical awareness of materials and validating of information built into lessons.
- Pupils will use age-appropriate tools to research Internet content.

Managing Information Systems

How will information systems security be maintained?

- Updating virus protection regularly.
- The Computing Subject Leader/network manager will review system capacity and security regularly.
- User logins and passwords are required to access the school network.
- Personal data sent over the Internet or taken off site will be encrypted.

How will email be managed?

- Use school email accounts only for professional purposes.
- Pupils must immediately tell a teacher if they receive offensive messages on Purple Mash
- Pupils must not reveal personal details of themselves or others in email communication, or arrange to meet anyone without specific permission from an adult.

How will published content be managed?

- The website contact details are the school address, email and telephone number. Staff or pupils' personal information must not be published.
- The head teacher will take overall editorial responsibility for online content published by the school and will ensure that content published is accurate and appropriate.
- Guidelines for publications, intellectual property rights, privacy policies and copyright will be adhered to.

Can pupils' images or work be published?

Yes, but:

- Pupils' photographs will not be published with their names.
- Written permission from parents or carers will be obtained and kept by the school before images/videos of pupils are published and high profile use of images e.g. on leaflets, website, banners etc. should be confirmed with the parent and added to the form with a date of verbal acceptance.

How will social networking, social media and personal publishing be managed?

All staff should be made aware of the potential risks of using social networking sites or personal publishing either professionally with students or personally. They should be made aware of the importance of considering the material they post, ensuring profiles are secured and how publishing unsuitable material may affect their professional status.

- Access to social media and social networking sites is controlled by the school's internet filters.
- Pupils will be advised never to give out personal details of any kind which may identify them and/or their location. See also the Staff Contact Policy.
- Social Media tools used in the classroom will be risk assessed before use.
- Staff personal use of social networking, social media and personal publishing sites will be discussed as part of staff induction and safe and professional behaviour will be outlined in the school Acceptable Use Policy.
- Pupils will be advised on security and privacy online and concerns regarding students' use of social networking, social media and personal publishing sites (in or out of school) will be raised with their parents/carers, particularly when concerning students' underage use of sites (see also what if? guide in appendix).
- Staff should not use social media to "sound off" about their day or staff/children. Social media to share teaching and learning experiences e.g. discussing resources used etc. is acceptable, but opinions should not relate to the school in any way.

How will filtering be managed?

- The school's broadband access includes filtering appropriate to the age and maturity of pupils and the school's filtering policy will be regularly reviewed by the eSafety team, with changes being risk assessed and with consent from the SLT where appropriate.
- Any breaches of filtering (e.g. inappropriate content) will be reported to the Head Teacher and logged. All members of the school community (all staff and all pupils) will be aware of this procedure.
- The School Senior Leadership Team and the eSafety team will meet regularly to review the eSafety log, including CPOMS incidents and check that any necessary changes are made to ensure that the filtering methods selected are effective.
- The school's access strategy will be designed by educators to suit the age and curriculum requirements of the pupils, with advice from network managers.

How will videoconferencing be managed?

- The use of videoconferencing with children will be planned and confirmed by the Head Teacher or Senior Leadership.
- Teachers to refer to a crib-sheet for reminding the other party about house rules etc.

How are emerging technologies managed?

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Pupils will be instructed about safe and appropriate use of personal devices both on and off site in accordance with the school Acceptable Use or Mobile Phone Policy.

How should personal data be protected?

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998. (See also the school's Data Protection Policy).

- GDPR

Policy Decisions

How will Internet access be authorised?

- All staff will read and sign the School Acceptable Use Policy before using any school ICT resources.
- Parents will be asked to read the School Acceptable Use Policy for pupils and discuss it with their child, where appropriate.
- All visitors to the school site who require access to the schools network or internet access will be asked to read and sign an Acceptable Use Policy.
- Parents will be informed that pupils will be provided with supervised Internet access appropriate to their age and ability.
- When considering access for vulnerable members of the school community (such as with children with special education needs) the school will make decisions based on the specific needs and understanding of the pupil(s).
- At Key Stage 1 pupils' access to the Internet will be by adult demonstration with and by children being directed to appropriate sites through favourites and shortcuts and age-appropriate search engines.
- At Key Stage 2 pupils will be supervised. Pupils will use age-appropriate search engines and online tools and online activities will be teacher-directed where necessary.

How will risks be assessed?
The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer. Neither the school nor the LEA can accept liability for the material accessed, or any consequences resulting from Internet use.

- The school's eSafety team, in conjunction with the Head Teacher/SLT will regularly meet and review the e–Safety policy, to ensure it is adequate and being implemented appropriately. They will identify, assess and ensure methods are in place to minimise risks.
- A risk assessment will be carried out and reviewed annually, or sooner in event of an issue arising.

How will the school respond to any incidents of concern?

- All members of the school community will be informed about the procedure for reporting e-Safety concerns (such as breaches of filtering, cyberbullying, cyber-crime, abuse, illegal content etc).
- The e-Safety Lead and/or the eSafety team will record all reported incidents and actions taken in the School e-Safety incident log and in any other relevant areas e.g. Bullying or Child protection on CPOMS.
- The Designated Child Protection Coordinator will be informed of any e-Safety incidents involving Child Protection concerns, which will then be escalated appropriately.
- The school will manage e-Safety incidents in accordance with the school discipline/ behaviour policy where appropriate. Staff to refer to 'what if' sheet for common eSafety issues (see appendix.)
- The school will inform parents/carers of any incidents of concern as and when required. After any investigations are completed, the school/eSafety team will debrief, identify lessons learnt and implement any changes required and if necessary, contact the Area Children's Safeguard Team or e-Safety officer and escalate the concern to the Police.

How will e–Safety complaints be handled?

- Complaints about Internet misuse will be dealt with under the School's complaints procedure and any issues (including sanctions) will be dealt with according to the school's disciplinary, behaviour and child protection procedures.
- All e-Safety complaints and incidents will be recorded by the school, including any actions taken.
- Pupils and parents will be informed of the complaints procedure and will need to work in partnership with the school to resolve issues.
- All members of the school community will be reminded about safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos online which cause harm, distress or offence to any other members of the school community.

How will Cyberbullying be managed?

- Cyberbullying (along with all other forms of bullying) of any member of the school community will not be tolerated. Full details are set out in the school's policy on anti-bullying and behaviour.
- All incidents of cyberbullying reported to the school will be recorded on CPOMS.
- Evidence will be gathered and stored before the article is deleted.

Sanctions for those involved in cyberbullying may include:

- The bully will be asked to remove any material deemed to be inappropriate or a service provider may be contacted to remove content if the bully refuses or is unable to delete content.
- Internet access may be suspended at school for the user for a period of time. Other sanctions for pupils and staff may also be used in accordance to the schools anti-bullying, behaviour policy or Acceptable Use Policy.
- Parent/carers of pupils will be informed.
- The Police will be contacted if a criminal offence is suspected.

How will learning platforms (LPs) be managed?

Pupils will have log ins and access to Mathletics, Reading Eggs and Purple Mash, Times Table Rockstars, Developing Experts, Class Dojo paid for and subscribed for by the school.

- SLT and staff will regularly monitor the usage of the LPs by pupils and staff in all areas, in particular message and communication tools and publishing facilities.
- Pupils/staff will be advised about acceptable conduct and use when using the LPs.
- Only members of the current pupil, parent/carers and staff community will have access to the LPs.
- All users will be mindful of copyright issues and will only upload appropriate content onto the LPs.
- When staff, pupils etc leave the school their account or rights to specific school areas will be disabled or transferred to their new establishment.
- Any concerns about content on the LPs may be recorded and dealt with in the following ways:

a) The user will be asked to remove any material deemed to be inappropriate or offensive.
b) The material will be removed by the site administrator if the user does not comply.
c) Access to the LPs for the user may be suspended.
d) The user will need to discuss the issues with a member of SLT before reinstatement.
e) A pupil's parent/carer may be informed.

- A visitor may be invited onto the LPs by a member of the SLT. In this instance there may be an agreed focus or a limited time slot.
- Pupils may require editorial approval from a member of staff. This may be given to the pupil to fulfil a specific aim and may have a limited time frame.

Remote Learning

- The school will ensure that children are able to learn remotely when they need to. In the event of school closure, class closures and individual self-isolation, the school provides a number of high-quality online resources parents and pupils can access (see Learning Platforms above).
- These remote learning platforms are safeguarded by individual pupil passwords and link directly to the class teacher (no third parties have access or share information). Passwords should not be shared with anyone outside your household.
- Teachers regularly monitor these platforms to mark and comment on pupil work. Uploading content and commenting on work is controlled by the class teacher. Content should be strictly school based and these online platforms should not be used to communicate or share content with other pupils.
- Live lessons will be conducted over Zoom and pupils/parents will receive an invite to these sessions from the class teacher. Pupils should follow the code of conduct for Live lessons (see Zoom guide).
- Access to the platform is made through the parent/carers account.
- An appropriate adult, like a parent or carer, is to remain in the room with the children whilst the meeting takes place. Parents and carers must show their face to the teacher before the meeting so they know an adult is nearby.

- Children must take part in the video call in a suitable communal environment (not a bedroom) and be appropriately dressed (uniform is not necessary, but they should be fully dressed in clothing that covers the top and bottom half of the body). All members of the household must be aware that the call is taking place and make sure they use appropriate language and behaviour when nearby or in the background. Some of the video calling software has a built-in option to 'blur' the background – parents are made aware of this if they feel this is an appropriate feature to turn on.
- Parents must make sure the child has 'logged off' the call correctly and signed out before turning off any devices.
- Parents will not contact teachers via Zoom outside of these pre-arranged calls. If contact needs to be made, this is through the normal contact procedures (i.e. emailing, Class Dojo)
- There are a limited number of devices available for children who do not have access at home to borrow from the school. These devices are remotely managed by the school including internet filtering. The devices are subject to an acceptable use agreement which is set by the school and signed by the parent/carer of the child borrowing the device. These devices remain the property of the school.
- Class Dojo is used as a means of contact between parents and children during Remote Learning and when in school. Parents are able to upload work their children have completed remotely to their child's portfolio and this is approved by the class teacher. Parents sign up to a user agreement before accessing Class Dojo and the school reserves the right to remove parents' access if the user agreement is broken.
- Messages sent between parents and teachers must be appropriate and teachers will only be available during working hours. The user agreement states:
    - Teachers will update the class stories on a weekly basis with information and some photographs showing what has been happening in class and only children who we have photo permission for will be included in the photographs in the class story.
    - Only parents/carers of children in that class can see the class story – parents cannot see other classes that they are not connected to.
    - Class teachers will only be logged into Class Dojo during the school day and in term time.
    - Class teachers will access Class Dojo at times throughout the school day. They will respond to messages when it is appropriate to do so which will not be guaranteed to be the same day.
    - Urgent messages should still be telephoned into the school office.
    - **All users will not share any photos on Social Media -** By signing up to the agreement, parents are agreeing not to share the images sent in any way for example on Social Media platforms such as Facebook, Instagram and WhatsApp.

How will mobile phones and personal devices be managed?

- The use of mobile phones and other personal devices by students that can send or receive communication or take photographs is not allowed in school, this includes smart watches and other smart technology.

Pupils Use of Personal Devices

- If a pupil breaches the school policy then the phone or device will be confiscated and will be held in a secure place in the school office. Mobile phones and devices will be released to parents/carers in accordance with the school policy.
- If a pupil needs to contact his/her parents/carers they will be allowed to use a school phone or the school office will contact the parent/carer for them.

Staff Use of Personal Devices

- Staff are not permitted to use their own personal phones or devices for contacting children, young people and their families within or outside of the setting in a professional capacity.
- Staff should not use personal devices such as mobile phones or cameras to take photos or videos of pupils and will only use work-provided equipment for this purpose.
- If a member of staff breaches the school policy then disciplinary action may be taken.

Communication Policy

- All users will be informed that network and Internet use will be monitored.
- An e–Safety training programme/scheme of work will be established across the school to raise the awareness and importance of safe and responsible internet use amongst pupils.
- e-Safety rules or copies of the student Acceptable Use Policy will be posted in all rooms with Internet access and responsible use of the Internet and technology will be encouraged across the curriculum.

How will the policy be discussed with staff?

- The e–Safety Policy will be formally provided to and discussed with all members of staff.
- To protect all staff and pupils, the school will implement Acceptable Use Policies.
- Staff will be made aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Up-to-date and appropriate staff training in safe and responsible Internet use, both professionally and personally, will be provided for all members of staff.
- The e-Safety team will highlight useful online tools which staff should use with children in the classroom. These tools will vary according to the age and ability of the pupils.
- All members of staff will be made aware that their online conduct out of school could have an impact on their role and reputation within school. Civil, legal or disciplinary action could be taken if they are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.

How will parents' support be enlisted?

- Parents' attention will be drawn to the school e–Safety Policy in newsletters, the school prospectus and on the school website.
- A partnership approach to e-Safety at home and at school with parents will be encouraged. This may include offering parent evenings with demonstrations and suggestions for safe home Internet use, or highlighting e–Safety at other attended events e.g. parent evenings.
- Parents, alongside pupils, will be requested to sign a Safety/Internet agreement as part of the Home School Agreement.
- Parents will be encouraged to read the school Acceptable Use Policy for pupils and discuss its implications with their children.
- Information and guidance for parents on e–Safety will be made available to parents in a variety of formats.

What ifs...
Please remember that this is not a “straight jacket” to adhere rigorously to, these guidelines will help to prompt and inform your unique response.
This guide forms part of the eSafety policy for Beardall Fields Primary and Nursery School.

An inappropriate website is accessed unintentionally by a pupil or member of staff.

1. Play the situation down; don’t make it into a drama. Ask the pupil to turn off the monitor, minimise the webpage or close the laptop lid, so the image or text cannot be seen by other pupils in the class. Make a note of the web address in the URL bar.
2. Discuss why the site is inappropriate with the pupil, or any issues that their experience might raise.
3. Report to the Headteacher as soon after the event as is reasonably possible eg. break, lunchtime (essentially this must be before the pupils concerned leave to go home) and decide whether to inform parents of any additional pupils who viewed the site.
4. Record incident on CPOMS if it involves a pupil or make a log of the incident in the safety log if no pupils are involved. This should be shared at staff briefing if appropriate and inform the eSafety Lead.
5. Inform the school technician to ensure the site is filtered.
6. Technician informs the filtering service.

An inappropriate website is accessed intentionally by a student

1. Explain why they should not be viewing this content. Show them where to find the appropriate and relevant information they are searching for.
2. Refer to the Acceptable Use Policy that was signed by the student and parents/carers.
3. Preserve any evidence through print outs or screen capture.
4. Use the school behaviour policy to identify the line of action.
5. Inform parents/carers if necessary as this may be a pattern of negative behaviour which is going un-checked at home.
6. Inform the school technician to ensure the site is filtered if need be.
7. Technician informs the LA filtering service.
8. Log the incident on CPOMS, tagging in the eSafety lead and DSL team.

You observe another adult using IT equipment inappropriately on school premises (eg. viewing videos on You Tube which are clearly unsuitable, posting inappropriate images of themselves on a social network.)

1. Report the misuse immediately to a member of the SLT. Do not speculate or discuss the issue with other staff. Do not challenge the member of staff who you observed.
2. Technicians will be instructed to ensure that there is no further access to the PC or laptop (device) if the device is owned by Beardall Fields primary school. If the device is owned by the user eg. a mobile phone, the Headteacher and user of the device should negotiate how data can be obtained through the device, alternatively this can be obtained through the network use logs.
3. If the material is offensive but not illegal, the school should then:
    a. Remove the PC to a secure place
    b. Instigate an audit of all ICT equipment by the schools ICT technician to ensure there is no risk of pupils accessing inappropriate materials in the school.
    c. Identify the precise details of the material
    d. Take appropriate disciplinary action
    e. Refer the incidence to the Local Authority Designated Officer (LADO)
    f. Inform governors of the incident
4. In an extreme case where the material is of an illegal nature:
    a. Contact the local police or CEOP and follow their advice.
    b. If requested, remove the PC/equipment to a secure place and document what you have done.
5. Consider re-training and general staff awareness raising.

Malicious or threatening comments are posted on an Internet site about a student or member of staff.

1. Secure and preserve any evidence using screen capture or photographing a monitor or mobile phone.
2. Inform the SLT/eSafety team who will work with the member of staff to preserve the evidence and identify the comments which are upsetting for the member of staff.
3. Inform and request the comments be removed if the site is administered externally.
4. Send all the evidence to CEOP at www.ceop.gov.uk, take guidance over the nature of the comments.
5. Endeavour to trace the origin and inform police if appropriate, applying the behaviour policy or staff conduct expectations. Refer to the Acceptable Use policy and the Staff ICT policy.

You are concerned that a pupil's safety is at risk because you suspect someone is using communication technologies (such as social networking sites) to make inappropriate contact with the pupil.

1. Report to and discuss with the SLT/eSafety team as soon as possible, on the day of the incident and contact parents. Log all actions taken on CPOMS.
2. In partnership with parents/carers, advise the pupil on how to terminate the communication and save all evidence offering confidential support to do so if needed.
3. Consider taking action to report/suspend account ensuring evidence is retained, do not delete the social network account at this stage. Offer advice and direct support to parent re. setting up safe internet etc...
4. Contact CEOP http://www.ceop.gov.uk/ with parent and student and ask for advice.
5. With the SLT and advice from CEOP, consider the involvement of the police and social services.
6. Take steps to check actions have been successful in stopping inappropriate contact.

A member of staff overhears a conversation between two KS2 pupils. The conversation was meant to be private. One of the pupils mentions that she is meeting up with a girl tonight, who she met through a Facebook group.

1. Consider that the pupil may be at risk of meeting an adult stranger tonight, without parental knowledge who is masquerading as a primary pupil.
2. Inform the SLT/eSafety team and plan a response before the end of the school day on the day of the incident. If necessary it may be right to keep the pupil at school until a parent/carer can be contacted.
3. Contact home to ascertain whether the parents/carers are accompanying the pupil to meet their "online" friend.
4. The pupil is under 13 and has a Facebook account, whilst this is not illegal, check that the parents/carers are aware of this. The parents must be informed.
5. Log the incident on CPOMS and the actions which you have agreed.
6. Follow the child protection policy and procedures, contacting the Police or making a MASH referral if necessary.

A current student asks you to be their online friend on a social network such as Facebook.

1. Politely decline the students offer and explain the inappropriateness of the request.
2. The same should also apply for online gaming, text messaging and any other forms of communication.
3. Inform the SLT/eSafety team as soon as you return to work and make a note in the eSafety log.
4. Educate pupils and parents/carers around e-safety issues.

You suspect that a student is accessing the school computers through the use of your username and log in. You have no idea how this may have happened.

1. Immediately change your current password, by holding down the keys ctrl, alt, delete and select, 'Change a password'.
2. Report to the SLT/eSafety team.
3. Ask the school technician to check history of log ins.
4. If a pupil is found to have used a staff log in, remind them of the Acceptable Use Policy which they signed. Apply the behaviour policy.
5. Identify if there has been a breach of confidential data and inform the SLT/eSafety team if you suspect there may be. eg. has the student copied and transferred data from the Staff Shared drive to their Facebook account / memory stick / mobile phone?
6. Log the incident on CPOMS.

You wanted to take some photos of the students and their work and post these on the school website to celebrate their achievement

1. Check that every student has both options ticked in the Photograph policy consent form.
2. Take photo with work camera (not a personal camera from home).
3. Never identify the student in the photo with their name, if this can be viewed by the public (eg. it will be on the website). Read the 'Can pupils' images or work be published?' section of this policy to ensure full compliance.

You wanted to take some photos of the students and their work and post these Class Dojo to celebrate their achievement

1. Check with the school office that all students have permissions for Class Dojo (Class Story or School Story depending on where you are posting the photos – Class Story can only be seen by members of the class, School Story by all members of the school.)
2. Take photo with work camera (not a personal camera from home).
3. Never identify the student in the photo with their name.
4. Read the 'Can pupils' images or work be published?' section and the 'Class Dojo' section of this policy to ensure full compliance.

---

e-Safety Contacts and References

CEOP (Child Exploitation and Online Protection Centre): www.ceop.police.uk
Childline: www.childline.org.uk
Childnet: www.childnet.com
Click Clever Click Safe Campaign: http://clickcleverclicksafe.direct.gov.uk
Kidsmart: www.kidsmart.org.uk
Think U Know website: www.thinkuknow.co.uk
360 safe – e-safety self-review tool: http://www.360safe.org.uk/
East Midlands Cyber Secure: https://www.eastmidlandscybersecure.co.uk/
Be Internet Legends: https://beinternetawesome.withgoogle.com/en_uk/
Parent Zone: https://parentzone.org.uk/

Beardall Fields Primary and Nursery School

Pupil Acceptable Use Agreement/ eSafety Rules

- Check with an adult before you use the computer or device.
- Ask before you do!
- Think about messages before you send them – be polite!
- Make sure an adult is nearby to help you.
- Don't leave a computer or device logged on.
- If something upsets you, ask an adult.
- Read things carefully before you click.
- Never share your personal details, like your address, online.
- Make sure you keep passwords to yourself and only log on as yourself.
- Ask permission before you take a photo of someone.
- Don't download anything without permission.
- Don't send messages to, or arrange to meet up with, people that you don't know in real life.
- Carry computers and devices carefully.
- Treat technology carefully and with respect.
- Don't eat or drink near computers or devices.

Summary
Treat ICT equipment with care.
Be nice to people when using the internet eg. to send emails.
If something on the computer or device upsets you, tell an adult straight away.

Dear Parent/ Carer
ICT including the internet, e-mail and mobile technologies, etc has become an important part of learning in our school. We expect all children use ICT in a responsible way and help them to do this.

Please read and discuss these eSafety rules with your child and return the slip at the bottom of this page. If you have any concerns or would like some explanation please contact the Head Teacher.
This Acceptable Use Agreement is a summary of our eSafety Policy which is available in full on our website/on request.

Parent/ carer signature
We have discussed this and …….....(child name) agrees to follow the eSafety rules and to support the safe use of ICT at Beardall Fields Primary and Nursery School.

Parent/ Carer Signature ……

Pupil Signature ……

Class …… Date ……

Beardall Fields Primary and Nursery School
Staff and Governor Acceptable Use Agreement / Code of Conduct

ICT (including data) and the related technologies such as e-mail, the internet and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with the Head Teacher or the school eSafety lead.

- I will only use the school's email / Internet / Intranet / Learning Platform and any related technologies for professional purposes or for uses deemed 'reasonable' by the Head or Governing Body.
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities.
- I will only use the approved, secure email system(s) for any school business.
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role.
- I will not give out my own personal details, such as mobile phone number, personal e-mail address and social networking identities to pupils.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- I will report any accidental access to inappropriate materials to the Head Teacher or eSafety lead.
- I will not download any software or resources from the internet that can compromise the network, or is not adequately licensed.
- I will not install any hardware or software without permission of the Head Teacher or Computing Lead.
- I will not connect a computer or mobile device to the network that does not have an up-to-date version of anti-virus software.
- I will ensure that personal data (such as data held on MIS software) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Head or Governing Body. Personal or sensitive data taken off site must be encrypted.
- Images of pupils and/ or staff will only be taken, stored and used for professional purposes inline with school policy and with written consent of the parent, carer or staff member. Images will not be distributed outside the school network without the permission of the parent/ carer, member of staff or Head Teacher.
- I will not use personal digital cameras or mobile phones for taking or transferring images of pupils or colleagues without permission.
- I will respect copyright and intellectual property rights.
- I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.
- I will support and promote the school's e-Safety and Data Security policies and help pupils to be safe and responsible in their use of ICT and related technologies.
- I will ensure that I am aware of eSafety and digital safe-guarding issues and that they are appropriately embedded in my classroom practice.
- I will not allow unauthorised individuals to access the school's network, email or learning platform.
- I agree and accept that any computer, laptop or mobile device loaned to me by the school, is provided solely to support my professional responsibilities.
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to my Line Manager or Head Teacher.
- I understand that failure to comply with the Acceptable Usage Policy could lead to disciplinary action.

This Acceptable Use Agreement is a summary of our eSafety Policy which is available in full on our website/on request.

User Signature
I agree to follow this code of conduct and to support the safe and secure use of ICT throughout the school

Signature …….…… Date ……

Full Name ……..(printed)

Job title . . . . . .

Beardall Fields Primary and Nursery School
Visitor Acceptable Use Agreement / Code of Conduct

This policy is designed to ensure that all visitors that require internet and/or network access are aware of the code of conduct and expectations when using any form of ICT in school. All visitors requiring internet and/or network access are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with the Head Teacher or the school eSafety lead.

- I will only use the school's email / Internet / Intranet / Learning Platform and any related technologies for designated purposes or for uses deemed 'reasonable' by the Head or Governing Body.
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities.
- I understand that I am being given temporary access and my access will be removed when I leave the premises/access is no longer required.
- I will only use the approved, secure email system(s) for any school related business.
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role.
- I will not give out my own personal details, such as mobile phone number, personal e-mail address and social networking identities to pupils.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- I will report any accidental access to inappropriate materials to the Head Teacher or eSafety lead.
- I will not download any software or resources from the internet that can compromise the network, or is not adequately licensed.
- I will not install any hardware or software without permission of the Head Teacher or Computing Lead.
- I will not connect a computer or mobile device to the network that does not have an up-to-date version of anti-virus software.
- I will not use personal digital cameras or mobile phones for taking or transferring images of pupils or colleagues without permission.
- I will respect copyright and intellectual property rights.
- I will not allow unauthorised individuals to access the school's network, email or learning platform.
- I agree and accept that any computer, laptop or mobile device loaned to me by the school, is provided solely to support my professional responsibilities.
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to the Head Teacher or eSafety Lead.
- I understand that failure to comply with the Acceptable Usage Policy could lead to disciplinary action.

This Acceptable Use Agreement is a summary of our eSafety Policy which is available in full on our website/on request.

User Signature
I agree to follow this code of conduct and to support the safe and secure use of ICT throughout the school

Signature …….…… Date …….

Full Name ……..(printed)

Job title/role . . . . . .

eSafety Incident Recording Sheet

Date and Time Incident Occurred	
Class/Individuals involved	
Nature of Concern	
Details of Incident	
Reported to	