Beckers Green Primary School

E-Safety Policy

September 2024

Due for review: Sep 2026

Beckers Green Primary School is committed to safeguarding and promoting the welfare of children
and expects all staff and volunteers to share this commitment.

Computing in the 21st Century is seen as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, at Beckers Green we need to build in the use of these technologies in order to arm our young people with the skills to access life-long learning and employment.

E-safety involves pupils, staff, governors and parents making best use of technology, information, training and this policy to create and maintain a safe online and ICT environment for Beckers Green Primary School.

"As in any other area of life, children and young people are vulnerable and may expose themselves to danger - knowingly or unknowingly - when using the Internet and other digital technologies. Indeed, some young people may find themselves involved in activities which are inappropriate or possibly illegal."

From: Safeguarding Children in a Digital World. BECTA 2006

Our E-Safety Policy has been written by the school, following government guidance. It has been agreed by senior management and approved by governors.

- The school's E-Safety coordinator is Mrs J Ward.
- The Safeguarding Governor is Vicky Powell.
- The E-Safety Policy and its implementation shall be reviewed annually.
- The school's ICT technician is Michael Bowden.

Roles and Responsibilities

Governors:

Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. The role of the Safeguarding Governor will include:

- Regular meetings with the E-Safety Co-ordinator/Headteacher
- Monitoring of E Safety policy and its implementation

Headteacher and Senior Leaders:

- The Headteacher and deputy head teacher are responsible for ensuring the safety (including e-safety) of members of the school community, though the day-to-day responsibility for e-safety will be delegated to the ICT technician and Headteacher.
- The Headteacher/Senior Leaders are responsible for ensuring that the Computing lead and other relevant staff receive suitable CPD to enable them to carry out their e-safety roles and to train other colleagues, as relevant.

- The Headteacher/Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal e-safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- Ensures Internet Safety section of School website is up to date with advice and guidance for parents and carers.
- The Headteacher and Deputy Head should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff. E-Safety concerns are logged on the schools CPOMS system which allows ease of reporting to Governors and early identification of any trends.

ICT technician:

Takes day-to-day responsibility for e-safety issues and monitors access requests on school internet server.

The E-Safety Co-ordinator (headteacher):

- Has a leading role in establishing and reviewing the school e-safety policy/documents.
- Ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- Provides training and advice for staff.
- Liaises with school ICT technical staff.
- Is notified of reports of e-safety incidents inform future e-safety provision.

Teaching and Learning

The Internet is an essential element for education, business and social interaction. Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils, and so the school has a duty to provide pupils with quality Internet access as part of their learning experience:

- The school Internet access will be designed expressly for pupil use including appropriate content filtering.
- Pupils will be given clear objectives for Internet use and taught what use is acceptable and what is not.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation. This will include supporting pupils to make judgements about what they see online and not automatically assume that what they see is true, valid or acceptable. Covering this content will enable pupils to recognise the techniques that are often used to persuade or manipulate others.

- As part of the computing curriculum, all year groups have digital literacy units that focus on different elements of staying safe online. These units include topics from how to use a search engine, digital footprints and cyber bullying. This is taken from the National Centre for Computing education curriculum. We also use the JIGSAW curriculum for PSHE which includes sections on E safety.
- The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.
- Half termly input is delivered to all classes from year 1 from Project Evolve – focused on internet safety.

Through ICT we ensure that the school meets the needs of all, taking account of gender, ethnicity, culture, religion, language, sexual orientation, age, ability, disability and social circumstances. It is important that in this school we meet the diverse needs of pupils to ensure inclusion for all and that all pupils are prepared for full participation in a multi-ethnic society.

Pupils are taught in all lessons to be critically aware of the materials/content they access on-line and are guided to validate the accuracy of information. Staff have received Prevent training and are aware of the dangers of the internet as a grooming tool for extremism or sexual abuse.

Authorised Internet Access

By explicitly authorising use of the school's Internet access pupils, staff, governors and parents are provided with information relating to e-safety and agree to its use:

- Our code of conduct policy gives clear guidance to staff about appropriate use of social media and ICT.
- Parents will be informed that pupils will be provided with supervised Internet access and asked to sign and return a consent form for pupil access.
- Only authorised equipment, software and Internet access can be used within the school.

World Wide Web

The Internet opens up new opportunities and is becoming an essential part of the everyday world for children: learning, homework, sharing are some of the legitimate and beneficial uses. However, there are inappropriate and undesirable elements that must be managed:

- The school uses Smoothwall as a filtering system, however if staff or pupils discover unsuitable sites, the URL (address), time and content shall be reported to the teacher who will then record the incident on CPOMS which notifies the headteacher.

If the concern is of an urgent or serious nature the Headteacher should take immediate action.

- The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.
- Pupils will be taught to be critically aware of the materials they are shown and how to validate information before accepting its accuracy.

E-mail

- E-mail is a quick and easy method of communication, ensuring beneficial and appropriate usage is an important part of e-safety.
- Pupils may only use approved e-mail accounts on the school system ie.) TEAMS
- Pupils must immediately tell a teacher if they receive offensive e-mail, they can also report their concern electronically via TEAMS. The email goes straight to the class teacher.
- Pupils must not reveal personal details of themselves or others in e-mail communication or arrange to meet anyone without specific permission.
- TEAMS allows children to have their own email account.
- Access in school to external personal e-mail accounts is not allowed.
- E-mail sent to external organisations should be written carefully and authorised before sending, in the same way as a using outlook.
- Chain letters, spam, advertising and all other emails from unknown sources will be deleted without opening or forwarding.

Security and passwords

Pupils and staff should never share passwords and staff must never let pupils use a staff logon. Staff must always 'lock' the PC if they are going to leave it unattended (the picture mute or picture freeze option on a projector will allow an image to remain on the screen and also allow a PC to be 'locked').

Social Networking

- Social networking Internet sites (such as, Whatsapp, Facebook) provide facilities to chat and exchange information online. This online world is very different from the real one with the temptation to say and do things beyond usual face-to-face contact.
- Use of social networking sites and newsgroups in the school, is not allowed and will be blocked/filtered.
- Pupils will be advised never to give out personal details of any kind that may identify themselves, other pupils, their school or location. This will also include not using personal photographs and videos.
- Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils.

- Pupils will be encouraged to only interact with known friends, family and staff over the Internet and deny access to others.
- Parents, pupils and staff will be advised of the dangers of discussing pupils, staff or the school on social networking sites. The governors will consider taking legal action, where appropriate, to protect pupils and staff against cyber bullying and defamatory comments.

Reporting

All breaches of the e-safety policy need to be recorded on CPOMS and referenced as Esafety concern. The details of the user, date and incident should be reported.

Incidents which may lead to child protection issues need to be passed on to one of the Designated Teachers immediately – it is their responsibility to decide on appropriate action not the class teachers.

Allegations involving staff should be reported to the Headteacher. If the allegation is one of abuse then it should be handled according to the DFE document titled 'Dealing with allegations of abuse against teachers and other staff'. If necessary the local authority's LADO should be informed.

Evidence of incidents must be preserved and retained.

The curriculum will cover how pupils should report incidents (e.g. Ceop button, trusted adult, Childline)

Mobile Phones

Many new mobile phones have access to the Internet and picture and video messaging. Whilst these are the more advanced features, they present opportunities for unrestricted access to the Internet and sharing of images. There are risks of mobile bullying, or inappropriate contact.

- Pupils by permission of the Head teacher can bring mobile phones onto the school site where it is seen by the school and parents as a safety/precautionary use. These are handed into the school office at 8:45 and collected at the end of the day.
- The sending of abusive or inappropriate text messages is forbidden.
- Staff should always use the school phone to contact parents, unless an emergency and school phone not available.
- Staff including students and visitors are not permitted to access or use their mobile phones within the classroom. All staff, visitors and volunteers should ensure that their phones are stored safely away during the teaching day.

- Staff may use their mobile phones in the staffroom/one of the school offices.
- On trips staff mobiles are used for emergency only.

Digital/Video Cameras/Photographs

Pictures, videos and sound are transferred to the school network from ipads via Tapestry.

- Pupils will not use digital cameras or video equipment at school unless specifically authorised by staff.
- Publishing of images, video and sound will follow the policy set out in this document under 'Publishing Content'.
- Parents and carers are permitted to take photos/videos of their own children in school events. They are requested not to share photos/videos from school events on social networking sites.
- The Headteacher or a nominee will inform parent(s)/guardian(s) and others present at school events that photographs/videos may be taken on the basis that they are for private retention and not for publication in any manner

Staff should always use a school camera to capture images and should not use their personal devices.
Photos taken and stored by the school are subject to GDPR legislation.

Published Content and the School Website

The school website is a valuable source of information for parents and potential parents.

- Contact details on the Website will be the school address, e-mail and telephone number.
- Staff and pupils' personal information will not be published.
- The Headteacher or a nominee will take overall editorial responsibility and ensure that content is accurate and appropriate.
- Photographs and videos that include pupils will be selected carefully and will not enable individual pupils to be clearly identified.
- Pupils' full names will not be used in association with photographs.
- Consent from parents will be obtained before photographs of pupils are published on the school Website.
- Parents should only upload pictures of their own child/children onto social networking sites.

Information System Security

- School ICT systems capacity and security will be reviewed regularly.

- Virus protection will be installed and updated regularly.
- Security strategies will be discussed with the Trust.
- E-safety will be discussed with our ICT support and those arrangements incorporated into our agreement with them.

Protecting Personal Data

Personal data will be recorded, processed, transferred and made available according to GDPR 2018 and Freedom of Information Act.

Assessing Risk

The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. The school does not accept liability for the material accessed, or any consequences of Internet access. The school will audit ICT use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate.

Handling E-Safety Complaints

- Complaints of Internet misuse will be dealt with by a senior member of staff.
- Any complaint about staff misuse must be referred to the Headteacher.
- Complaints of a child protection nature shall be dealt with in accordance with school child protection procedures.
- Pupils and parents will be informed of the complaints procedure.
- Discussions will be held with the community police officer to establish procedures for handling potentially illegal issues.

Communication of Policy

Pupils:

- Rules for Internet access will be posted in all networked rooms.
- Pupils will be informed that Internet use will be monitored.
- Pupils will be informed of the importance of being safe on social networking sites. This will be strongly reinforced across all year groups during Computing lessons, PSHE and weekly Project Evolve sessions. All year groups look at different areas of safety through the digital literacy lessons.

Staff:

- All staff will be given the School e-safety Policy and its importance explained. The code of Conduct also refers to online platforms and usage.

Parents:

- Parents' attention will be drawn to the School e-safety Policy in newsletters and on the school Website.

Further Resources

We have found these web sites useful for e-safety advice and information.

http://www.thinkuknow.co.uk/	Set up by the Police with lots of information for parents and staff including a place to report abuse.
http://www.childnet-int.org/	Non-profit organisation working with others to "help make the Internet a great and safe place for children".
www.net-aware.org.uk	Includes information on latest games and apps which may be harmful to children.
https://www.ceop.police.uk/CEOP-Reporting/	Enables children and parents to report concerns

RESPONSIBLE USE OF EMAIL AND THE INTERNET

- I will ask permission before entering any Web site, unless my teacher has already approved that site.
- I will use only my own login and password, which I will keep secret.
- I will only e-mail people I know, or my teacher has approved.
- The messages I send will be polite and sensible.
- When sending e-mail, I will not give my home address or phone number, or arrange to meet someone.
- I will ask for permission before opening an e-mail and or e-mail attachment sent by someone I do not know.
- I will not use Internet chat except if it is in a discussion room that has been set up by my teacher using TEAMS.
- Any work I display using TEAMS will be work that I know I would want my family and friends to see.
- If I see anything I am unhappy with or I receive messages I do not like, I will tell my teacher immediately.
- I know that the school may check my computer files and may monitor the Internet sites I visit.
- I understand that if I deliberately break these rules, I would be stopped from using the Internet or computers.

Pupil's Agreement

I have read and understand the school Rules for Responsible use of TEAMS and the Internet. I will use TEAMS and the Internet in a responsible way and obey these rules at all times. In particular, I will not

share my password with anybody else. I will not give out my name, home address or phone number in e-mail messages or write messages that I would not let my teachers and parents read. If I receive an e-mail which upsets me or an e-mail from somebody I don't know, I will tell my teacher immediately.

Child's Signature: …… Date: ……...

Parent's Consent for Internet Access and use of email

I have read and understood the school rules for Responsible Use of TEAMS and the Internet, and give permission for my son/daughter to access this via the Internet. I understand that the school will take all reasonable precautions to ensure pupils cannot access inappropriate materials. I understand that the school cannot be held responsible for the nature or content of materials accessed through the Internet.

I agree that should my son/daughter need to access TEAMS at home or anywhere else, I agree that I will take all reasonable precautions to ensure my son/daughter cannot access inappropriate materials and that he/she will use their desktop in an appropriate manner.

I agree that my son/daughter's work may be published on TEAMS or the school website.

I will try to ensure that my child understands the importance of keeping their password a secret.

Parent's Signature: …… Date: ……..

This form is valid for the period of time your child attends Beckers Green Primary School. Please contact the school at any time if you wish to withdraw your consent.

Signed:…… (Parent/Carer) Relationship to Child: ……

Name: ……. Date: ……