BUTTERWICK PINCHBECK'S ENDOWED CHURCH OF ENGLAND PRIMARY SCHOOL

E-SAFETY POLICY

Date agreed: November 2017
Date to be reviewed: November 2018

BUTTERWICK PINCHBECK'S ENDOWED CHURCH OF ENGLAND PRIMARY SCHOOL

E-Safety Policy

E-safety Co-ordinator: Mr Tom Huck

Headteacher: Mrs Sam Towers

Chair of Governors: Mrs Louise Pearson

E-Safety encompasses Internet technologies and electronic communications such as mobile phones, laptops, tablets etc. It highlights the need to educate pupils about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience.

The school's E-Safety policy will operate in conjunction with and relate to other policies including those for Behaviour, Anti-Bullying, Curriculum, Acceptable Use policy, Data Protection and Security, ICT and Safeguarding.

E-Safety depends on effective practice at a number of levels:

- Responsible ICT use by all staff and students; encouraged by education and made explicit through published policies.
- Sound implementation of E-Safety policy in both administration and the curriculum, including the secure school network design and use.
- Safe and secure broadband that is filtered via F1 Group and monitored via Future Digital Solutions using their Policy Central monitoring software.

Our E-Safety Policy has been written by the school, building on the South West Grid for Learning advice website for E-Safety, local authority and government guidance and in conjunction with teaching and support staff, pupils and parents. It has been agreed by senior management and approved by Governors and teachers.

- The E-Safety Coordinator is Mr. Huck, who is also one of the school's Child Protection Officers and a member of the Senior Leadership Team. He is also assisted by Miss Smith; the ICT Co-ordinator.
- Governors responsible for monitoring E-safety are Helen Dower and Louise Pearson
- The E-Safety Policy and its implementation will be reviewed annually, or in response to an e safety incident.

Roles and Responsibilities:

The following section outlines the E-safety roles and responsibilities of individuals and groups within Butterwick Primary School.

Governors:

The governing body is accountable for ensuring that our school has effective policies and procedures in place; as such they will:

- Review this policy at least annually and in response to any e-safety incident to ensure that the policy is up to date, covers all aspects of technology use within the school, to ensure e-safety incidents were appropriately dealt with and ensure the policy was effective in managing those incidents.

- Appoint at least one governor to have overall responsibility for the governance of e-safety at the school who will have termly meetings with the E-safety coordinator to monitor E-safety incident logs, identified training needs and to keep up to date with emerging risks and threats through technology use and report back at Governor meetings.

Headteacher:
The Headteacher has a duty of care 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 E-Safety Co-ordinator

- The Headteacher and at least another member of the SLT 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.
- The Headteacher is responsible for ensuring that the E-Safety Co-ordinator and other relevant staff receive suitable training to enable them to carry out their E-safety roles and to train other colleagues.
- The Headteacher 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.
- All e-safety incidents are dealt with promptly and appropriately.

E-Safety Co-ordinator, in conjunction with ICT coordinator and other staff:
The role of the E-Safety Co-ordinator will:

- Take day to day responsibility for E-safety issues as well as reviewing the school E-safety and acceptable use policies.
- Ensure all staff are aware of the procedures that need to be followed in the event of an E-safety incident taking place.
- Provide training and advice for staff and pupils.
- Conduct questionnaires with pupils on an annual basis.
- Liaise with the Local Authority, Policy Central and the F1 group (our monitoring and filtering providers) to ensure the internet filtering and monitoring system is working well, inappropriate websites are blocked and to deal with any issues that may arise through inappropriate use of the internet by staff or pupils.
- Receive reports of any E-safety incidents involving staff or pupils and create a log of incidents to inform future E-safety needs or developments.
- Meet regularly with the E-Safety Governor and feed back to the relevant committee at Governors meetings.
- Report regularly to the SLT.
- Ensure all staff have read and signed the Acceptable Use Policy
- Ensure that the e safety curriculum is being followed across the whole school
- Induct new staff in this policy, e safety curriculum and the reporting arrangements

ICT Co-ordinator, in conjunction with the E-safety officer and other staff:
Will include:

- Ensuring that the school's technical infrastructure is not open to misuse or malicious attack by liaising with the school internet provider.
- Ensuring that the school meets required E-safety technical requirements.
- Ensuring that users may only access the networks and devices through a properly enforced password protection policy.
- Making sure they have an up to date awareness of E-safety matters and of the current E-safety policy and practices.

- Ensuring that they have read, understood and signed the Staff Acceptable Use Policy.
- Ensuring that they report any suspected misuse or problem to the Headteacher/E-safety Coordinator.

Teaching and Support Staff:
The role of the teaching and support staff will include:

- Having an up to date awareness of E-safety matters and of the current school E-safety policy and practices.
- Ensuring they have read, understood and signed the Staff Acceptable Use Policy.
- Reporting any suspected misuse or problem to the E-Safety Coordinator and/or Headteacher for investigation, action and possible sanctions.
- Teach e safety across the school using the 360 e safety curriculum and the 'jigsaw' PSHE curriculum as well as regularly reminding children of their responsibilities when using the internet in other subjects.
- All digital communications with pupils, parents, carers should be on a professional level and only carried out using official school systems.
- Ensuring pupils understand and follow the E-safety and Acceptable Use Policies
- Ensuring pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- Internet access will be planned to enrich and extend learning activities. Access levels will be reviewed to reflect the curriculum requirements and age of pupils.
- Staff should guide pupils in on-line activities that will support the learning outcomes planned for the pupils' age and maturity
- Monitoring the use of digital technologies, mobile devices, cameras etc. in lessons and other school activities (where allowed) and implement current policies with regard to these devices. 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.
- In a perfect world, inappropriate material would not be visible to pupils using the Internet, but this is not easy to achieve and cannot be guaranteed. Pupils may occasionally be confronted with inappropriate material, despite all attempts at filtering. Pupils should be taught what to do if they experience material that they find distasteful, uncomfortable or threatening. For example: to close or minimise the page and report the incident immediately to the teacher.

Pupils:

- Are responsible for using the school digital technology systems in accordance with the Acceptable Use Policy (AUP) for Pupils
- Staff will discuss the acceptable use policy with the children, who will then sign the AUP.
- Have an understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so, whilst at school or outside of school.
- Should understand the importance of adopting good E-safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of school, if it is related to their membership of the school.

Parents:
Parents/Carers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way. We will offer parent sessions, run by Dan Hawbrook, (Lincolnshire's E-safety Advisor) giving an opportunity to find out how children use technology, possible pitfalls, safety rules, guidance, advice and support for using the internet at home.

We will encourage parents to support the school in promoting good E-safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- access to parents' sections of the school website

Parents' attention will be drawn to the school E–Safety Policy in newsletters, the school prospectus and on the school website. Information, advice and guidance on useful resources and websites for parents on E–Safety are made available to parents on the school website. These are signposted via newsletters, this policy (see final page) and the school website.

- Parents will be encouraged to read the school's Acceptable Use Policy for pupils and discuss its implications with their children.

Teaching and Learning

Why is Internet use important?

- Internet use is part of the statutory curriculum and is a necessary tool for learning.
- The Internet is a part of everyday life for education, business and social interaction.
- The school has a duty to provide students with quality Internet access as part of their learning experience.
- Pupils use the Internet widely outside school and need to learn how to evaluate Internet information and to take care of their own safety and security.
- The purpose of Internet use in school is to help us raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management functions.
- Internet access is an entitlement for students who show a responsible and mature approach to its use.

How does Internet Use Benefit Education?
Benefits of using the Internet in education include:

- Access to worldwide educational resources including museums and art galleries;
- Inclusion in the National Education Network which connects all UK schools;
- Educational and cultural exchanges between pupils worldwide;
- Vocational, social and leisure use in libraries, clubs and at home;
- 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;
- Access to learning wherever and whenever convenient.

How will pupils learn how to evaluate Internet content?

- Pupils will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Pupils will use age-appropriate tools to research Internet content.

- The evaluation of online materials is a part of teaching and learning in every subject and will be viewed as a whole-school requirement across the curriculum.

Managing Information Systems:

1. **How will information systems security be maintained? Kier services maintain our system and we also use Policy central to monitor websites used by staff and pupils**
    - The security of the school information systems and users will be reviewed regularly.
    - Virus protection will be updated regularly.
    - Personal data sent over the Internet or taken off site should be encrypted.
    - Portable media may not used without specific permission.
    - Unapproved software will not be allowed in work areas or attached to email.
    - Files held on the school's network will be regularly checked.
    - The ICT coordinator will review system capacity regularly.
    - The use of user logins and passwords to access the school network will be enforced.
    - Pupils may only use approved email accounts for school purposes.
    - Pupils must immediately tell a designated member of staff if they receive offensive email.
    - Pupils must not reveal personal details of themselves or others in email communication, or arrange to meet anyone without specific permission from an adult.
    - Whole class or group email addresses will be used in primary schools for communication outside of the school.
    - Staff will only use official school provided email accounts to communicate with pupils and parents/carers, as approved by the Senior Leadership Team.
    - Access in school to external personal email accounts may be blocked.
    - Excessive social email use can interfere with learning and will be restricted.
    - Email sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on school headed paper would be.
    - The forwarding of chain messages is not permitted.
    - Staff should not use personal email accounts during school hours or for professional purposes.

2. **How will published content be managed?**
    - The contact details on the website should be the school address, email and telephone number. Staff or pupils' personal information must not be published.
    - The Headteacher will take overall editorial responsibility for online content published by the school and will ensure that content published is accurate and appropriate.
    - The school website will comply with the school's guidelines for publications including respect for intellectual property rights, privacy policies and copyright.

3. **Can pupils' images or work be published?**
    Images or videos that include pupils will be selected carefully and will not provide material that could be reused.
    - Pupils' full names will not be used anywhere on the website, particularly in association with photographs.

- Written permission from parents or carers will be obtained before images/videos of pupils are electronically published.
- Pupils work can only be published with their permission or the parents.
- Written consent will be kept by the school where pupils' images are used for publicity purposes, until the image is no longer in use.
- The school will have a policy regarding the use of photographic images of children which outlines policies and procedures.

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

- The school system does not allow access to social media and social networking sites.
- Pupils will be advised never to give out personal details of any kind which may identify them and/or their location. Examples would include real name, address, mobile or landline phone numbers, school attended, IM and email addresses, full names of friends/family, specific interests and clubs etc.
- Staff official blogs or wikis should be password protected and run from the school website with approval from the Senior Leadership Team. Members of staff are advised not to run social network spaces for pupil use on a personal basis.
- Personal publishing will be taught via age appropriate sites that are suitable for educational purposes. They will be moderated by the school where possible.
- Pupils will be advised on security and privacy online and will be encouraged to set passwords, deny access to unknown individuals and to block unwanted communications.
- All members of the school community are advised not to publish specific and detailed private thoughts, especially those that may be considered threatening, hurtful or defamatory.
- Any 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, if it is a cause for concern.
- 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's Acceptable Use Policy.

5. How will filtering be managed?

- The school's broadband access will include filtering appropriate to the age and maturity of pupils.
- The school will work with F1 group (formerly Mouchel) to ensure that filtering is continually reviewed.
- The school will have a clear procedure for reporting breaches of filtering. All members of the school community (all staff and all pupils) will be aware of this procedure. School use Policy Central software to monitor staff and pupil internet use.
- If staff or pupils discover unsuitable sites, the URL will be reported to the School E-Safety Coordinator who will then record the incident and escalate the concern as appropriate.
- Changes to the school filtering policy will be risk assessed by staff with educational and technical experience prior to any changes and where appropriate with consent from the Senior Leadership Team.
- The School Senior Leadership Team will ensure that regular checks are made to ensure that the filtering methods selected are effective. Weekly reports are made available from Policy Central

- Any material that the school believes is illegal will be reported to appropriate agencies.

6. How are emerging technologies managed?

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out by the staff team 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 Policy.

7. How should personal data be protected?

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

8. How will Internet access be authorised?

- The school, will maintain a current record of all staff and pupils who are granted access to the school's electronic communications via F1 Group.
- All staff will read and sign the School Acceptable Use Policy before using any school ICT resources.
- Pupils will discuss, read and sign the School Acceptable Use Policy on joining our school. Staff will discuss with pupils and renew each new school year.
- All visitors to the school site who require access to the schools network will be given a temporary log in. Staff should not allow visitors to use their own staff log in and password
- 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 occasional directly supervised access to specific and approved online materials.
- 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.

9. 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. The school cannot accept liability for the material accessed, or any consequences resulting from Internet use.
- 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.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990 and breaches will be reported.
- Methods to identify, assess and minimise risks will be reviewed regularly.

10. 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, illegal content etc.)
- The E-Safety Coordinator will record all reported incidents and actions taken in the School E-Safety incident log and other in any relevant areas e.g. Bullying or Child protection log, emails to Kier re websites that have been reported and subsequently blocked.
- 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.
- The school will inform parents/carers of any incidents of concerns as and when required.
- After any investigations are completed, the school will debrief, identify lessons learnt and implement any changes required.
- Where there is cause for concern or fear that illegal activity has taken place or is taking place then the school will contact the Children's Safeguard Team or E-Safety officer and escalate the concern to the Police
- If the school is unsure how to proceed with any incidents of concern, then the incident may be escalated to the County E-Safety Officer.
- If an incident of concern needs to be passed beyond the school then the concern will be escalated to the E-Safety officer.

11. How will e–Safety complaints be handled?

- Any complaint about staff misuse will be referred to the Headteacher.
- All e–Safety complaints and incidents will be recorded by the school, including any actions taken.
- Parents and pupils will need to work in partnership with the school to resolve any issues.
- All members of the school community will need to be aware of the importance of confidentiality and the need to follow the official school procedures for reporting concerns.
- Discussions will be held with the Children's Safeguarding Team to establish procedures for handling potentially illegal issues.
- Any issues (including sanctions) will be dealt with according to the school's disciplinary, behaviour and child protection procedures.
- 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.

12. How is the Internet used across the community?

- The school will be sensitive to Internet-related issues experienced by pupils out of school, e.g. social networking sites, and offer appropriate advice.
- The school will provide appropriate levels of supervision for students who use the internet and technology whilst on the school site.

13. 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.

- Pupils, staff and parents/carers will be advised to keep a record of the bullying as evidence.
- The school will take steps to identify the bully, where possible and appropriate. This may include examining school system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police, if necessary.
- Pupils, staff and parents/carers will be required to work with the school to support the approach to Cyberbullying and the school's E-Safety ethos.

14. 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.

15. How will mobile phones and personal devices be managed?

- The use of mobile phones and other personal devices by students are not allowed in our school
- The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the school community and any breaches will be dealt with as part of the school discipline/behaviour policy.
- School staff may confiscate a phone or device if they believe it is being used to contravene the schools behaviour or bullying policy. The phone or device might be searched by the Senior Leadership team with the consent of the pupil or parent/carer. If there is suspicion that the material on the mobile may provide evidence relating to a criminal offence the phone will be handed over to the police for further investigation.
- Mobile phones and personal devices will not be used during lessons or formal school time by staff.
- Mobile phones will not be used during lessons or formal school time unless as part of an approved and directed curriculum based activity with consent from a member of staff.
- Electronic devices of all kinds that are brought in to school are the responsibility of the user. The school accepts no responsibility for the loss, theft or damage of such items. Nor will the school accept responsibility for any adverse health effects caused by any such devices either potential or actual.
- Mobile phones and personal devices are not permitted to be used in certain areas within the school site such as changing rooms, toilets and swimming pools, unless in an emergency.

16. Pupils Use of Personal Devices

- Pupils are not allowed the use of mobile phones in school. If they are accidentally brought in to school, pupils will hand them in and they will be kept in the school office until the end of the school day
- If a pupil needs to contact his/her parents/carers they will be allowed to use a school phone

- 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 unless in an emergency e.g. school trips
- Mobile Phone and devices will be switched off or switched to 'silent' mode, Bluetooth communication should be "hidden" or switched off and mobile phones or devices will not be used during teaching periods unless permission has been given by a member of Senior Leadership Team in emergency circumstances. If members of staff have an educational reason to allow children to use mobile phones or personal device as part of an educational activity then it will only take place when approved by the Senior Leadership Team.
- 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.

17. Other:

- All users will be informed that network and Internet use will be monitored
- An e–Safety curriculum will be taught across the school to raise the awareness and importance of safe and responsible internet use amongst pupils. Safe and responsible use of the Internet and technology will be reinforced across the curriculum and subject areas.
- Pupil instruction regarding responsible and safe use will precede Internet access.
- Staff will regularly remind pupils of E-Safety rules and the student Acceptable Use Policy.
- Particular attention to E-Safety education will be given where pupils are considered to be vulnerable.

18. 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 is monitored and traced to the individual user.

19. 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.
- Staff who manage filtering systems or monitor ICT use will be supervised by the Senior Leadership Team and have clear procedures for reporting issues.
- The School 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.

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
Cybermentors: www.cybermentors.org.uk
Digizen: www.digizen.org.uk
Internet Watch Foundation (IWF): www.iwf.org.uk
Kidsmart: www.kidsmart.org.uk
Think U Know website: www.thinkuknow.co.uk
Virtual Global Taskforce — Report Abuse: www.virtualglobaltaskforce.com