Cuckney C of E Primary School
E-Safety Policy

Name of Publication	**E-Safety Policy**
Date of Issue	**May 2018**
Author	**Lisa Crossland**
Responsibility for review	**Governing body**
Copies of documents are kept	**In the Head Teacher's policy folder**
Date Reviewed:	**May 2020**
Date Reviewed:	**November 2020-** *Updated to include E-safety during remote learning. R Worboys.*
Date Reviewed:	

Signed:

L C Crossland
Head teacher

Margaret Lovell
Chair of Governors

E-Safety Policy

Statement of intent

At Cuckney C of E Primary School, we understand that computer technology is an essential resource for supporting teaching and learning. The internet, and other digital and information technologies, open opportunities for pupils and play an important role in their everyday lives.

Whilst our school recognises the importance of promoting the use of computer technology throughout the curriculum, we also understand the need for safe internet access and appropriate use.

Our school has created this policy with the aim of ensuring appropriate and safe use of the internet and other digital technology devices by all pupils and staff.

The school is committed to providing a safe learning and teaching environment for all pupils and staff, and has implemented important controls to prevent any harmful risks.

1. Legal framework

1.1. This policy has due regard to the following legislation, including, but not limited to:

- Human Rights Act 1998
- Data Protection Act 1998
- Freedom of Information Act 2000
- Regulation of Investigatory Powers Act 2000
- Safeguarding Vulnerable Groups Act 2006
- Education and Inspections Act 2006
- Computer Misuse Act 1990, amended by the Police and Justice Act 2006
- Communications Act 2003
- Protection of Children Act 1978
- Protection from Harassment Act 1997

1.2. This policy also has regard to the following statutory guidance:

- DfE (2016) 'Keeping children safe in education'

1.3. This policy will be used in conjunction with the following school policies and procedures:

- Safeguarding Policy
- Anti-Bullying Policy
- Social Media Policy
- ICT Curriculum Policy

2. Use of the internet

2.1. The school understands that using the internet is important when raising educational standards, promoting pupil achievement and enhancing teaching and learning.

2.2. Internet use is embedded in the statutory curriculum and is therefore an entitlement for all pupils, though there are many controls the school is required to implement to minimise harmful risks.

2.3. When accessing the internet, individuals are especially vulnerable to several risks which may be physically and emotionally harmful, including:

- Access to illegal, harmful or inappropriate images
- Cyber bullying
- Access to, or loss of, personal information
- Access to unsuitable online videos or games
- Loss of personal images
- Inappropriate communication with others
- Illegal downloading of files
- Exposure to explicit or harmful content, e.g. involving radicalisation
- Plagiarism and copyright infringement
- Sharing the personal information of others without the individual's consent or knowledge

3. Roles and responsibilities

3.1. It is the responsibility of all staff to be alert to possible harm to pupils or staff due to inappropriate internet access or use, both inside and outside of the school, and to deal with incidents of such as a priority.

3.2. The school are responsible for ensuring that there are appropriate filtering and monitoring systems in place to safeguard pupils.

3.3. Class teachers and support staff are responsible for ensuring the day-to-day e-safety in the school, and managing any issues that may arise, with the support of the headteacher if necessary.

3.4. The headteacher will provide all relevant training and advice for members of staff as part of the requirement for staff to undergo regularly updated safeguarding training and be able to teach pupils about online safety.

3.5. Class teachers will regularly monitor the provision of e-safety in the school and will provide feedback to the headteacher.

3.6. Any e-safety reports and incidents, such as inappropriate internet use, involving either pupils or staff, must be logged and submitted to the headteacher, where appropriate action will be taken at the discretion of the headteacher and the Chair of Governors. The headteacher will keep a log of all incidents reported.

3.7. The headteacher will attempt to find alternatives to monitoring staff use of social media, where possible, and will justify all instances of monitoring to ensure that it is necessary and outweighs the need for privacy. The member of staff who is being monitored will be consulted prior to any interception by the school.

3.8. Cyber bullying incidents will be reported in accordance with the school's Anti-Bullying Policy.

3.9. The governing body will hold meetings with the headteacher to discuss the effectiveness of the e-safety provision, current issues, and to review incident logs, as part of the school's duty of care.

3.10. The ICT co-ordinator, headteacher and governing body will evaluate and review this E-Safety Policy on an annual basis, taking into account the latest developments in ICT and the feedback from staff/pupils.

3.11. The ICT co-ordinator will review and amend this policy with the headteacher, considering new legislation, government guidance and previously reported incidents, to improve procedures.

3.12. Teachers are responsible for ensuring that e-safety issues are embedded in the curriculum and safe internet access is promoted at all times.

3.13. All staff are responsible for ensuring they are up-to-date with current e-safety issues, and this E-Safety Policy.

3.14. Parents are responsible for ensuring their child understands how to use computer technology and other digital devices appropriately.

3.15. The headteacher is responsible for communicating with parents regularly and updating them on current e-safety issues and control measures.

3.16. All pupils are aware of their responsibilities regarding the use of school-based ICT systems and equipment, including their expected behaviour.

4. E-safety education

4.1. **Educating pupils:**

- Age appropriate e-safety will be taught across the curriculum on a regular basis, ensuring that pupils are aware of the safe use of new technology both inside and outside of the school.
- Pupils will be taught about the importance of e-safety and are encouraged to be critically aware of the content they access online, including extremist material and the validity of website content.
- Clear guidance on the rules of internet use will be presented in all classrooms.
- Pupils are instructed to report any suspicious use of the internet and digital devices.
- PSHE lessons and themed weeks will be used to educate pupils about cyber bullying, including how to report cyber bullying, the social effects of spending too much time online and where to access help.
- The school will hold e-safety events, such as Safer Internet Day and Anti Bullying Week, to promote online safety.

4.2. **Educating staff:**

- E-safety training opportunities are available to all staff members, including whole school activities and CPD training courses.
- All staff will undergo e-safety training on a yearly basis to ensure they are aware of current e-safety issues and any changes to the provision of e-safety, as well as current developments in social media and the internet.
- All staff will undergo regular audits by the ICT co-ordinator to identify areas of training need.
- All staff will employ methods of good practice and act as role models for pupils when using the internet and other digital devices.
- All staff will be educated on which sites are deemed appropriate and inappropriate.
- All staff are reminded of the importance of acknowledging information they access online, to avoid copyright infringement and/or plagiarism.
- Any new staff are required to fully understand and agree to act within this E-Safety Policy.
- The headteacher will act as the first point of contact for staff requiring e-safety advice.

4.3. **Educating parents:**

- E-safety information will be directly delivered to parents through a variety of formats, including newsletters, the school website and social media.
- Twilight courses/presentations will be run by the school for parents.
- Parents' evenings, meetings and other similar occasions will be utilised to inform parents of any e-safety related concerns.

5. E-safety control measures

5.1. **Internet access:**

- Management systems will be in place to allow teachers and members of staff to control workstations and monitor pupils' activity.
- Effective filtering systems from Nottinghamshire County Council are established to eradicate any potential risks to pupils through access to, or trying to access, certain websites which are harmful or use inappropriate material.
- Filtering systems will be used which are relevant to pupils' age ranges, their frequency of use of ICT systems, and the proportionality of costs compared to risks.
- The governing body will ensure that use of appropriate filters and monitoring systems does not lead to 'over blocking', such that there are unreasonable restrictions as to what pupils can be taught with regards to online teaching and safeguarding.
- Any requests by staff for websites to be added or removed from the filtering list must be first authorised by the headteacher, before being put forward to Nottinghamshire County Council. Please refer to the appendices in the school Social Media Policy for the relevant reporting documentation.
- All school systems will be protected by up-to-date virus software.

- An agreed procedure will be in place for the provision of temporary users, e.g. volunteers and trainees.
- Master users' passwords will be available to the headteacher for regular monitoring of activity.
- Staff can use the internet for personal use during out-of-school hours, as well as break and lunch times.
- Personal use will only be monitored by the headteacher for access to any inappropriate or explicit sites, where it is justifiable to be necessary and in doing so, would outweigh the need for privacy.
- Inappropriate internet access by staff may result in the staff member being permitted to use the internet for school purposes only and prohibited from using any personal devices. This will be dealt with following the process outlined in section 7.4 of this policy.

5.2. **Email:**

- Staff will be given approved school email accounts and must use these accounts for work-related purposes only.
- The use of personal email accounts to send and receive personal data or information, or for any work-related correspondence is prohibited.
- No sensitive personal data shall be sent to any other pupils, staff or third parties via email.
- Staff members are aware that their email messages are not monitored, however can be accessed, with prior consent, should any concerns arise.
- Pupils are not to have access to email correspondence in school, unless approved by the headteacher and monitored by the class teacher.
- Any emails sent by pupils to external organisations will be overseen by their class teacher and must be authorised before sending.
- Chain letters, spam and all other emails from unknown sources will be deleted without opening.

5.3. **Social networking:**

- Use of social media on behalf of the school will be conducted following the processes outlined in our Social Media Policy.
- Access to social networking sites will be filtered as appropriate.
- Pupils are regularly educated on the implications of posting personal data online outside of the school.
- Staff are regularly educated on posting inappropriate photos or information online, which may potentially affect their position and the school as a whole.
- Staff are not permitted to communicate with pupils over social networking sites and are reminded to alter their privacy settings.
- Staff are not permitted to publish comments about the school which may affect its reputability.
- The use of school linked social media sites are permitted under the rules and regulations set out in our Social Media Policy.

5.4. **Published content on the school website and images:**

- The headteacher will be responsible for the overall content of the website and will ensure the content is appropriate and accurate.
- Contact details on the school website will include the phone number, email and address of the school – no personal details of staff or pupils will be published.
- Images, videos and full names of pupils, or any content that may easily identify a pupil, will be selected carefully, and will not be posted until authorisation from parents has been received.
- Staff should ensure that they familiarise themselves with parental consents regarding the publishing of such content listed above using the school's Scholar Pack system.
- Pupils are not permitted to take or publish photos of others without permission from the individual.
- Staff are able to take pictures, though they must do so in accordance with school policies in terms of the sharing and distribution of such. Staff will not take pictures using their personal equipment, unless approved by the headteacher prior to use.
- Any member of staff that is representing the school online, e.g. through blogging, must express neutral opinions and not disclose any confidential information regarding the school, or any information that may affect its reputability.

5.5. **Mobile devices and hand-held computers:**

- The headteacher may authorise the use of mobile devices by a pupil where it is seen to be for safety or precautionary use.
- Pupils are not permitted to access the school's Wi-Fi system at any times using their mobile devices and hand-held computers.
- Mobile devices are not permitted to be used during school hours by pupils.
- The sending of inappropriate messages or images from mobile devices is prohibited.
- The school will be especially alert to instances of cyber bullying and will treat such instances as a matter of high priority.

5.6. **Virus management:**

- Technical security features, such as virus software, are kept up-to-date and managed by the headteacher.
- The ICT co-ordinator will ensure that the filtering of websites and downloads is up-to-date and monitored.

6. Online safety during remote learning

6.1. This section of the policy will be enacted in conjunction with the school's E Safety Policy.

6.2. Where possible, all interactions will be textual and public.

6.3. When using **video communication**, all staff and pupils must:

- Communicate in groups – one-to-one sessions are not permitted.
- Wear suitable clothing – this includes others in their household.
- Be situated in a suitable 'public' living area within the home with an appropriate background – 'private' living areas within the home, such as bedrooms, are not permitted during video communication.
- Use appropriate language – this includes others in their household.
- Maintain the standard of behaviour expected in school.
- Use the necessary equipment and computer programs as intended.
- Not record, store, or distribute video material without permission.
- Ensure they have a stable connection to avoid disruption to lessons.
- Always remain aware that they are visible.

6.4. When using **audio communication,** all staff and pupils must:

- Use appropriate language – this includes others in their household.
- Maintain the standard of behaviour expected in school.
- Use the necessary equipment and computer programs as intended.
- Not record, store, or distribute audio material without permission.
- Ensure they have a stable connection to avoid disruption to lessons.
- Always remain aware that they can be heard.

6.5. Pupils not using devices or software as intended will be disciplined in line with the Behavioural Policy.

6.6. The school will risk assess the technology used for remote learning prior to use and ensure that there are no privacy issues or scope for inappropriate use.

6.7. The school will consult with parents as soon as possible prior to the period of remote learning about what methods of delivering remote teaching are most suitable – alternate arrangements will be made where necessary.

6.8. The school will ensure that all school-owned equipment and technology used for remote learning has suitable anti-virus software installed, can establish secure connections, can recover lost work, and allows for audio and visual material to be recorded or downloaded, where required.

6.9. During the period of remote learning, the school will maintain regular contact with parents to:

- Reinforce the importance of children staying safe online.
- Ensure parents are aware of what their children are being asked to do, e.g. sites they have been asked to use and staff they will interact with.
- Encourage them to set age-appropriate parental controls on devices and internet filters to block malicious websites.
- Direct parents to useful resources to help them keep their children safe online.

6.10. The school will not be responsible for providing access to the internet off the school premises and will not be responsible for providing online safety software, e.g. anti-virus software, on devices not owned by the school.

7. Cyber bullying

7.1. For the purpose of this policy, cyber bullying is a form of bullying whereby an individual is the victim of harmful or offensive posting of information or images online.

7.2. The school recognises that both staff and pupils may experience cyber bullying and will commit to preventing any instances that should occur.

7.3. The school will regularly educate staff, pupils and parents on the importance of staying safe online, as well as being considerate to what they post online.

7.4. Pupils will be educated about online safety through teaching and learning opportunities as part of a broad and balanced curriculum; this includes covering relevant issues within PSHE lessons as well as sex and relationship education.

7.5. The school will commit to creating a learning and teaching environment which is free from harassment and bullying, ensuring the happiness of all members of staff and pupils.

7.6. The school has zero tolerance for cyber bullying, and any incidents will be treated with the upmost seriousness and will be dealt with in accordance with our Anti-Bullying Policy.

7.7. The headteacher will decide whether it is appropriate to notify the police or anti-social behaviour coordinator in their LA of the action taken against a pupil.

8. Reporting misuse

8.1. Cuckney C of E Primary School will clearly define what is classed as inappropriate behaviour in the Acceptable Use Agreement (Appendix 1), ensuring all pupils and staff members are aware of what behaviour is expected of them.

8.2. Inappropriate activities are discussed and the reasoning behind prohibiting activities due to e-safety are explained to pupils as part of the curriculum in order to promote responsible internet use.

8.3. **Misuse by pupils:**

- Teachers have the power to discipline pupils who engage in misbehaviour with regards to internet use.
- Any instances of misuse should be immediately reported to a member of staff, who will then report this to the headteacher, using the relevant reporting procedures.

- Any pupil who does not adhere to the rules outlined in our Acceptable Use Agreement and is found to be wilfully misusing the internet, will have a letter sent to their parents explaining the reason for suspending their internet use.
- Members of staff may decide to issue other forms of disciplinary action to a pupil upon the misuse of the internet. This will be discussed with the headteacher and will be issued once the pupil is on the school premises.
- Complaints of a child protection nature, such as when a pupil is found to be accessing extremist material, shall be dealt with in accordance with our Child Protection and Safeguarding Policy.

8.4. **Misuse by staff:**

- Any misuse of the internet by a member of staff should be immediately reported to the headteacher, using the relevant reporting procedures.
- The headteacher will deal with such incidents in accordance with the appropriate guidance and may decide to take disciplinary action against the member of staff.
- The headteacher will decide whether it is appropriate to notify the police or anti-social behaviour coordinator in their LA of the action taken against a member of staff.
- Where there is any misuse regarding the headteacher, the above procedures should be followed by the Chair of Governors.

8.5. **Use of illegal material:**

- In the event that illegal material is found on the school's network, or evidence suggest that illegal material has been accessed, the police will be contacted.
- Incidents will be immediately reported to the Internet Watch Foundation and the police will be contacted if the illegal material is, or is suspected to be, a child sexual abuse image hosted anywhere in the world, a non-photographic child sexual abuse image hosted in the UK, or criminally obscene adult content hosted in the UK.
- If a child protection incident is suspected, the school's child protection procedure will be followed.

9. Monitoring and review

9.1. The ICT co-ordinator and headteacher will evaluate and review this E-Safety Policy annually, taking into account the school's e-safety calendar, the latest developments in ICT and the feedback from staff/pupils.

9.2. This policy will also be reviewed on an annual basis by the governing body; any changes made to this policy will be communicated to all members of staff.

9.3. Members of staff are required to familiarise themselves with this policy as part of their induction programmes.

Appendix 1

Acceptable Use Agreement (Pupils and Parents)

E-safety rules

At Cuckney C of E Primary School, pupils **are expected to**:

- Only use ICT on the school premises for studying purposes.
- Make sure ICT communication with other pupils and adults is polite and responsible.
- Be responsible for their behaviour while using ICT.
- Inform their class teacher of anything they see online which makes them feel uncomfortable.
- Understand that their use of ICT can be checked and that parents/carers will be contacted if a member of school staff is concerned about a pupil's e-safety.
- Be careful when using computer equipment and treat it with respect.
- Abide by the rules regarding bringing personal devices into school.
- Seek the advice of a teacher before downloading material.

Pupils will **not**:

- Try to bypass the internet settings and filtering system.
- Use email without their teacher's consent.
- Share passwords.
- Delete or open other people's files and documents.
- Use other people's accounts.
- Send, use or view any content which is unpleasant. If something like this is found, such as inappropriate images or the use of offensive language, pupils will report it to their teacher.
- Share details of their name, phone number or address.
- Meet someone they have contacted online, unless it is part of a school project and/or a responsible adult is present.
- Upload images, sound, video or text content that could upset pupils, staff and others.
- Try to install software onto the school network.

Parents **will**:

- Support and uphold the school's rules regarding the use of school ICT systems.
- Act in accordance with the school's policy when using the internet in relation to the school, its employees and pupils.
- Only store and use images of pupils for school purposes, acting in line with the school's ICT Policy.

Remote learning rules

At Cuckney C of E Primary School, pupils **are expected to:**

- Adhere to this policy at all times during periods of remote learning.
- Ensure that their school work is completed on time and to the best of their ability.

- Report any technical issues to their parent/carer or class teacher as soon as possible.
- Notify a responsible adult if they are feeling unwell or are unable to complete the school work they have been set.
- Ensure they use any equipment and technology for remote learning as intended.
- Adhere to the school behavioural policy at all times.

During video communication

- Communicate in groups- one-to-one sessions are not permitted.
- Wear suitable clothing- this includes others in their household.
- Be situated in a suitable 'public' living area within the home with an appropriate background – 'private' living areas within the home, such as bedrooms, are not permitted during video communication.
- Use appropriate language – this includes others in their household.
- Maintain the standard of behaviour expected in school.
- Use the necessary equipment and computer programs as intended.
- Not record, store, or distribute video material without permission.
- Ensure they have a stable connection to avoid disruption to lessons.
- Always remain aware that they are visible.

During audio communication

- Use appropriate language – this includes others in their household.
- Maintain the standard of behaviour expected in school.
- Use the necessary equipment and computer programs as intended.
- Not record, store, or distribute audio material without permission.
- Ensure they have a stable connection to avoid disruption to lessons.
- Always remain aware that they can be heard.

Parents **are expected to**:

- Adhere to this policy at all times during periods of remote learning.
- Ensure their child is available to learn remotely at the times requested by the school, and that the school work set is completed on time and to the best of their child's ability.
- Report any technical issues to the school as soon as possible.
- Ensure that their child always has access to remote learning material provided by school.
- Report any absence to the relevant class teacher.
- Ensure their child uses the equipment and technology used for remote learning as intended.