Fritchley CE (Aided) Primary School

e-Safety Policy

Why does a School or Setting need an e-Safety Policy?

In today's society, children, young people and adults interact with technologies such as mobile phones, games consoles and the Internet on a daily basis and experience a wide range of opportunities, attitudes and situations. The exchange of ideas, social interaction and learning opportunities involved are greatly beneficial to all, but can occasionally place children, young people and adults in danger.

e-Safety covers issues relating to children and young people as well as adults and their safe use of the Internet, mobile phones and other electronic communications technologies, both in and out of school. It includes education for all members of the school community on risks and responsibilities and is part of the 'duty of care' which applies to everyone working with children.

Schools and other settings must decide on the right balance between controlling access to the internet and technology, setting rules and boundaries and educating students and staff about responsible use. Schools must be aware that children and staff cannot be completely prevented from being exposed to risks both on and offline. Children should be empowered and educated so that they are equipped with the skills to make safe and responsible decisions as well as to feel able to report any concerns. All members of staff need to be aware of the importance of good e-Safety practice in the classroom in order to educate and protect the children in their care. Members of staff also need to be informed about how to manage their own professional reputation online and demonstrate appropriate online behaviours compatible with their role.

Breaches of an e-Safety policy can and have led to civil, disciplinary and criminal action being taken against staff, pupils and members of the wider school community. It is crucial that all settings are aware of the offline consequences that online actions can have.

Schools must be aware of their legal obligations to safeguard and protect children on and offline and the accountability of these decisions will sit with the Head Teacher and the Governing body.

The e-Safety policy is essential in setting out how the school plans to develop and establish its e-Safety approach and to identify core principles which all members of the school community need to be aware of and understand.

1.1 Who will write and review the policy?

The Headteacher and Governing body have a legal responsibility to safeguard children and staff and this includes online activity. The school has appointed an e–Safety Coordinator, Mrs Esther Devonport, who will monitor e-safety in conjunction with Ms Karin Baker, Headteacher. The e–Safety Policy and its implementation will be reviewed in accordance with the cycle set by the governing body or whenever a technological development or issue arise resulting in this necessity. Our e–Safety Policy has been written by the school, building on the DCC e–Safety Policy and government guidance.

The policy has been agreed by the approved by governors who have appointed a member of the Governing Body to take lead responsibility for e-Safety

1.2 Teaching and learning

1.2.1 Why is Internet use important?

The rapid developments in electronic communications are having many effects on society. It is important that the children use the internet and other computing equipment as a necessary tool for learning as well as preparing them for adult working life. The school has a duty to provide students with quality internet access as part of their learning experience. The purpose of this is to raise educational standards, promote pupil achievement, to support the professional work of staff and to enhance the school's management functions.

1.2.2 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;
- improved access to technical support including remote management of networks and automatic system updates;
- access to learning wherever and whenever convenient.

1.2.3 How can Internet use enhance learning?

The school's Internet access will be designed to enhance and extend education. Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use. The schools will ensure that the copying and subsequent use of Internet-derived materials by staff and pupils complies with copyright law and learn how to reference this in use. Access levels to the internet will be reviewed to reflect the curriculum requirements and the age and ability of pupils. Staff should guide pupils to online activities that will support the learning outcomes planned for the pupils' age and ability.

1.2.4 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 through using 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.

1.3 Managing Information Systems

1.3.1 How will information systems security be maintained?

The Computer Technician, Mr Martyn Shaw, is primarily responsible for maintaining the school system against cyber attacks, however staff must be responsible and aware in terms of downloading material and educating children with regard to these dangers.

Areas for consideration by the Computer Technician:
Local Area Network (LAN) security issues include:

- Users must act reasonably — e.g. the downloading of large files during the working day will affect the service that others receive.
- Users must take responsibility for their network use. For DCC staff, flouting electronic use policy is regarded as a reason for dismissal.
- Workstations should be secured against user mistakes and deliberate actions.
- Servers must be located securely and physical access restricted.
- The server operating system must be secured and kept up to date.
- Virus protection for the whole network must be installed and current.

- Access by wireless devices must be proactively managed and secured with a minimum of WPA2 encryption.

Wide Area Network (WAN) security issues include:

- Central KPSN Schools Broadband firewalls and local CPEs are configured to prevent unauthorised access between schools.
- Decisions on WAN security are made on a partnership between schools and KCC/EiS.

The Schools Broadband network is protected by a cluster of high performance firewalls. These industry leading appliances are monitored and maintained by a specialist security command centre.

The security of the school information systems and users will be reviewed regularly and virus protection will be updated regularly. Personal data sent over the Internet or taken off site will be encrypted. Portable media may not used without specific permission followed by an anti-virus / malware scan which is the responsibility of the member of staff who is accessing it. Unapproved software will not be allowed in work areas or attached to email. The use of user logins and passwords to access the school network will be enforced. The Computer Technician will review system capacity regularly.

1.3.2 How will email be managed?

Pupil email

At present, pupils are accessing email via an internal email program, 2Simple email. This simulates the process of sending an email whilst staying within the network. During the teaching in these sessions, pupils are made aware of the dangers of external email and methods which they may use to protect themselves.

Staff email

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. 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.

1.3.3 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 head teacher 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. Staff email addresses may be published at their request.

1.3.4 Can pupils' images or work be published?

Images or videos that include pupils will be selected carefully and will endeavour not to provide material that could be reused. Pupils' full names will not be used anywhere on the website or social media. The names of children shall not be associated with photos and particular care should be taken in relation to publishing photos where named certificates are being held. Written permission from parents or carers will be obtained before images/videos of pupils are electronically published in the form of an initial contract upon the child's entry to school.

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

Access to all social networking sites is blocked through the CCS system therefore accessing this kind of material within school should be exceedingly rare. However, children will be advised how to communicate safely using social networking. 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 Headteacher. Members of staff are not permitted 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. 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. 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.

1.3.6 How will filtering be managed?

The filter settings at school are set by CCS and are on a medium setting in line with guidance from Derbyshire County Council. It is important that schools recognise that filtering is not 100% effective, for example during an image search. Occasionally mistakes may happen and inappropriate content may be accessed. It is therefore important that children should always be supervised when using internet access and that Acceptable Use Policies are in place. In addition, Internet Safety Rules should be displayed, and both children and adults should be educated about the risks online. There should also be an Incident Log to report breaches of filtering or inappropriate content being accessed. Procedures need to be established to report such incidents to parents and DCC where appropriate.

Any material that the school believes is illegal must be reported to appropriate agencies such as Derbyshire Police or CEOP.

Teachers should always evaluate any websites/search engines before using them with their students; this includes websites shown in class as well as websites accessed directly by the pupils. Often this will mean checking the websites, search results etc just before the lesson. Remember that a site considered safe one day may be changed due to the Internet being a dynamic entity. Particular attention should also be paid to advertisements as they can change each time the web page is accessed.

1.3.7 How will videoconferencing be managed?

At present Fritchley Primary and Nursery School does not have the facility to videoconference. When this becomes applicable this area of the policy will be amended.

1.3.8 How are emerging technologies managed?

Schools should keep up to date with new technologies, including those relating to mobile phones and handheld devices, and be ready to develop appropriate strategies. For instance text messaging via mobile phones is a frequent activity for many pupils and families; this could be used to communicate a pupil's absence or send reminders for exam coursework. There are dangers for staff however if personal phones are used to contact pupils and therefore a school owned phone should be issued.

The inclusion of inappropriate language or images is difficult for staff to detect. Pupils may need reminding that such use is inappropriate and conflicts with school policy. Abusive messages should be dealt with under the school's behaviour and/or anti-bullying policies.

1.3.9 How should personal data be protected?

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

1.4 Policy Decisions

1.4.1 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. All staff will read and sign the Acceptable Use Policy before using any school Computing resources.

Parents will be asked to read the School Acceptable Use Policy for pupil access and discuss it with their child, where appropriate. Parents will be informed that pupils will be provided with supervised Internet access appropriate to their age and ability.

According to Setting Type

- 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.

1.4.2 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 DCC can accept liability for the material accessed, or any consequences resulting from Internet use. The school will audit computer use to establish if the e–Safety policy is adequate and that the implementation of the e–Safety policy is appropriate.

1.4.3 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.
- 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, indentify 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 Area Children's Officer or 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 to communicate to other schools in Derbyshire.

1.4.4 How will e–Safety complaints be handled?

Complaints about Internet misuse will be dealt with under the School's complaints procedure. Any complaint about staff misuse will be referred to the head teacher. All e–Safety complaints and incidents will be recorded by the school, including any actions taken. This can be done in the e-safety log in the cabinet in the computer room. Pupils and parents will be informed of the complaints procedure. 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.

1.4.5 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.

1.4.6 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.
- There are clear procedures in place to support anyone in the school community affected by cyberbullying.
- All incidents of cyberbullying reported to the school will be recorded.
- There will be clear procedures in place to investigate incidents or allegations of Cyberbullying.
- 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.
- 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.

1.4.7 How will mobile phones and personal devices be managed?

- The use of mobile phones for students is strictly prohibited during the school day.
- 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.
- 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.

Staff Use of Personal Devices/Accounts

- 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 are able to use the school phone where contact with pupils or parents/carers is required.
- Mobile Phones and devices will be 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.
- Staff should not use personal social media accounts to comment on school social media accounts. Likewise, they should not use the school Facebook or other social media accounts to comment on personal accounts.
- If a member of staff breaches the school policy then disciplinary action may be taken.

1.5 Communication Policy

1.5.1 How will the policy be introduced to pupils?

- At the beginning of the academic year, each class will have a dedicated e-safety session.
- Primarily, all aspects of e-safety will be taught to the children through their weekly computing sessions in relation to the Switched On Computing scheme of work.
- E safety will be addressed at the beginning of any session involving computers/technology whether accessing the internet or not.
- Additional useful e–Safety programmes include:
  - Think U Know: www.thinkuknow.co.uk
  - Childnet: www.childnet.com
  - Kidsmart: www.kidsmart.org.uk
  - Orange Education: www.orange.co.uk/education
  - Safe: www.safesocialnetworking.org

- All users will be informed that network and Internet use will be monitored.
- Particular attention to e-Safety education will be given where pupils are considered to be vulnerable.

1.5.2 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.

1.5.3 How will parents' support be enlisted?

- Parents' attention will be drawn to the school e–Safety Policy in newsletters, the school prospectus, school website and school social media accounts.
- Parents will be requested to discuss the child acceptable use policy with their child as part of the Home School Agreement.

The School e-Safety Coordinator is **Mrs Esther Devonport**

Policy approved by Head Teacher: …… Date: ……

Policy approved by Governing Body: …….. (Chair of Governors)

Date: ……

The date for the next policy review is **January 2020**

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

Cybermentors: www.cybermentors.org.uk

Digizen: www.digizen.org.uk

Internet Watch Foundation (IWF): www.iwf.org.uk

Kidsmart: www.kidsmart.org.uk

Teach Today: http://en.teachtoday.eu

Think U Know website: www.thinkuknow.co.uk

Virtual Global Taskforce — Report Abuse: www.virtualglobaltaskforce.com