Chapel End Infant School
&
Early Years Centre

E-Safety Policy
2015

Policy written: June 2015
To be reviewed: July 2017

Signed ______________________________ Headteacher (Mrs Terri Martin)

Signed ______________________________ Chair of Governors (Mr Terry Toomey)

Aims of Chapel End Infant School & Early Years Centre

"Caring, sharing, trying our best"

At Chapel End Infant School & Early Years Centre we aim to provide a safe, caring and stimulating environment, which offers opportunities:-

- For access to a broad and balanced curriculum that promotes the fulfilment of each child's academic, creative and physical potential and fosters their social, moral and spiritual values.
- For everyone within the school to have a sense of wonder, an enthusiasm for learning and help children to develop as independent thinkers and learners with enquiring minds.
- For children to learn to be organized, confident and persistent individuals and to develop a respect and understanding for others.
- For the development of positive relationships between all members of the school community to support and enhance children's learning.

Equal opportunities

At Chapel End Infant School & Early Years Centre school we believe that every child is entitled to equal access to the curriculum, regardless of race, gender, class or disability.

Inclusion

We are committed to promoting learning and teaching environments for all, which embraces the values of inclusive educational practices.

Through a child-centred approach, we aim to ensure that education is accessible and relevant to all our learners. At Chapel End Infant School & Early Years Centre we respect each other and celebrate diversity and difference.

Chapel End Infant School & Early Years Centre
E-Safety Policy

Contents

Appendices

Chapel End Infant School & Early Years Centre School

E-Safety Policy June 2013

1．Who will write and review the policy?

The school will appoint an e–Safety Coordinator. The Policy will be written and reviewed annually by the e-safety Coordinator with input from the head teacher, staff and governors together with guidance received from LGfL policy and government guidance.

2．Why is Internet use important?

- Internet use is part of the national curriculum and 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 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.

3．How does the Internet use benefit education?

Benefits of using the Internet in education include:

- access to worldwide educational resources including museums and art galleries;
- 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, effective curriculum practice and online training courses.
- 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 (e.g. homework, independent topic research, revision)

4. How can Internet use enhance learning?

- The school's Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of the pupils.
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Internet access will be planned to enrich and extend learning activities.
- Access levels reflect the curriculum requirements and age of pupils.
- Staff should guide pupils in online activities that will support the learning outcomes planned for the pupils' age and maturity.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- Pupils will be made aware of the need to acknowledge the source of information used and to respect copyright when using Internet material in their own work.

5. Authorised Internet Access

- The school will maintain a current record of all staff and pupils who are granted Internet access.
- All staff must read and sign the 'Staff Information Systems Code of Conduct' before using any school ICT resource.
- Parents will be informed that pupils will be provided with supervised Internet access.
- Parents will be asked to sign and return a consent form for pupil access.

6. How will pupils learn how to evaluate Internet content?

- If staff or pupils discover unsuitable sites, the URL (address) and content must be reported to the Local Authority helpdesk via the e-safety coordinator or network manager.
- The school should ensure that the use of Internet derived materials by staff and pupils complies with copyright law.
- Pupils should be taught to be critically aware of the materials they read and be shown how to accept and validate information before accepting its accuracy.
- Pupils will be made aware of the need to acknowledge the source of information and to respect copyright when using Internet material in their own work.

7. Information System Security

- The security of the school information systems and users will be reviewed regularly. The school uses robust security provision and a managed educational network service through LGfL.
- Files held on the school's network will be subject to checks.

- The ICT Subject Leader/ICT Support Manager will review system capacity regularly.
- Sensitive information relating to individuals should be saved onto the school network or onto an encrypted memory stick, not saved onto a laptop.

8. Email use in school

- Pupils may only use approved email accounts on the school system.
- Pupils must immediately tell a teacher if they receive an 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 for communication outside of the school.
- Email sent to external organisations must be written carefully in the same way as a letter written on school headed paper.
- The forwarding of chain messages is not permitted.
- Staff should only use school email accounts for school related communication.

9. Published content and the School Website

- The contact details shown on the school's website are that of the school. This will also include the school's email address and telephone number. Staff or pupils' personal information will not be published.
- The head teacher will take overall editorial responsibility and ensure that content is accurate and appropriate.
- The website will comply with the school's guidelines for publications including respect for intellectual property rights and copyright.
- Uploading of information to the schools website is in the main the responsibility of the Head Teacher, Terri Martin and Administration Officers, Angela Clarke and Joan Smith. All teaching staff have access to the website and can upload relevant documents to their class pages.

10. Publishing Pupils' Images and Work

- The school will use images of children on the school website only under the direction of the Head Teacher. A record of children whose images may not be used on the website is held in the school office. All staff must refer to this list before publishing any images of children. No children's names will be published alongside photographs on the school website.
- Images that include pupils will be carefully selected.

- Parents must inform the school office if they do not want images of their child/ren to be electronically published.
- Pupils work will be published without pupils names assigned.
- Digital images/videos of pupils must be stored on the specifically allocated drive on the school network, not on individual laptops or tablets. All photographs will be deleted at the end of the year unless specifically required for a key school publication.

11. Photographs/Video taken by parents/carers for personal use

- In the event of parents/carers wanting to take photographs of children e.g. at school performances or on school trips, they are reminded that these are for their own private retention and not for publication in any manner including social networking sites such as Facebook. Parents/carers will be reminded of this policy at school performances.

12. Social Networking – Pupils

- The use of social media presents new and interesting opportunities and enables anyone with a computer and internet connection the quick and easy ability to publish opinion and information, and listen to and engage with those who read it. Social Networking sites include, but are not exclusively, Facebook, Twitter, Email, Blogs, Linked-In, You tube, MySpace and Bebo.
- Within school the access to social media and social networking sites will be controlled.
- 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.
- Pupils should be advised not to place personal photos on any social network space. They should consider how public the information is and consider using private areas. Advice should be given regarding background detail in a photograph which could identify the student or his/her location.
- If personal publishing is to be used with pupils then it must use age appropriate sites suitable for educational purposes. Personal information must not be published and the site should be moderated by school staff.
- Pupils will be advised on security and encouraged to set passwords, deny access to unknown individuals and be instructed how to block unwanted communications. Pupils will be encouraged to invite known friends only and deny access to others by making profiles private.
- Pupils are advised not to publish specific and detailed private thoughts, especially those that may be considered threatening, hurtful or defamatory.
- E-safety workshops will be arranged by the e-safety coordinator for staff, pupils and parents on a regular basis.

- Pupils and parents will be informed that pupils under 14 years of age should not be accessing social networking sites such as Facebook.

13. Social Networking – staff, governors and parents/carers

- Staff official blogs or wikis will be password protected.
- Alongside the opportunities offered by social networking sites, it must be recognised that there are risks attached to the use of social media as the distribution of material cannot be controlled. Once posted to an initial target audience, material can be posted anywhere through the networks of each individual in that audience and beyond. Therefore, staff and governors are expected to conduct themselves in any social media forum as they would in school.
- Staff are also reminded to adhere to the guidelines regarding photographs of children for their own private retention. It is inappropriate for staff to ‘friend’ a child of primary school age.
- Staff, governors and parents/carers are reminded that social media sites should not be used as a forum for public debate, complaint or grievance regarding school issues and they should refer to the appropriate complaints or grievance policy.

14. Cyber bullying

Cyber bullying is bullying through the use of communication technology like mobile phone text messages, emails or websites. This can take many forms for example:

- Sending threatening or abusive text messages or emails, personally or anonymously
- Making insulting comments about someone on a website, social networking site (e.g facebook)
- Making or sharing derogatory or embarrassing videos of someone via mobile phone or email

Chapel End Infant School & Early Years Centre School will not tolerate any form of cyber bullying, (whether inside or outside school) to another pupil or member of staff or governor and may take further action against any individual concerned.

15. Filtering

- The school will work with LGfL and SBS (ICT Technicians) to ensure that systems to protect pupils and staff are continually reviewed and improved.

- If staff or pupils discover unsuitable sites, the URL must be reported to the e–Safety Coordinator.

- The school's broadband access will include filtering appropriate to the age and maturity of pupils.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

- Any material that the school believes is illegal must be reported to appropriate agencies such as IWF or CEOP.
- The school's access strategy will be designed by educators to suit the age and curriculum requirements of the pupils, with advice from network managers.

16. Videoconferencing

- When this becomes available in the school, videoconferencing will use the educational broadband network to ensure quality of service and security rather than the Internet.
- Videoconferencing will be appropriately supervised for the pupils' age.

17. Managing Emerging Technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Mobile phones will not be used during lessons or formal school time.
- The sending of abusive or inappropriate text, picture or video messages is forbidden.

18. Protecting Personal Data

- Personal data will be recorded, processed transferred and made available according to the Data Protection Act 2003.

19. Assessing Risks

- The school will take all reasonable precautions to prevent access to appropriate 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. Neither the school nor the Local Authority can accept liability for the material accessed, or 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.

20. 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 Head Teacher.
- Complaints of a child protection nature must be dealt with in accordance

with child protection and safeguarding procedures.

- Pupils and parents will be informed of the complaints procedure.

21. Communication of Policy

Pupils

- Rules for Internet access will be posted in all classrooms.
- Pupils will be informed that Internet use will be monitored.

Staff & Governors

- All staff will be given the School e-Safety Policy and its importance explained.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

Parents

- Parents’ attention will be drawn to the School e-Safety Policy, in newsletters, in the school prospectus and on the school web site.

CHAPEL END

E-Safety Rules for Key Stage 1

'Think then Click'

These rules help us to stay safe on the Internet

- We only use the Internet when an adult is with us.
- We can click on the buttons or links when we know what they do.
- We can search the Internet with an adult.
- We always ask if we get lost on the Internet.
- We can send and open emails together.
- We can write polite and friendly emails to people that we know.

Chapel End Infant School & Early Years Centre
E-Safety Rules

Please read our full e-safety policy on the school website
www.chapelendinfants.com

These e-safety rules help to protect pupils and the school by describing acceptable and unacceptable computer use.

- The school owns the computer network and can set rules for its use.
- It is a criminal offence to use a computer or network for a purpose not permitted by the school.
- Irresponsible use may result in the loss of network or Internet access.
- Network access must be made via the user's authorised account and password, which must not be given to any other person.
- All network and Internet use must be appropriate to education.
- Copyright and intellectual property rights must be respected.
- Messages shall be written carefully and politely, particularly as email could be forwarded to unintended readers.
- Anonymous messages and chain letters are not permitted.
- Users must take care not to reveal personal information through email, personal publishing, blogs or messaging.

The school may exercise its right to monitor the use of the school's computer systems, including access to websites, the interception of email and the deletion of inappropriate materials where it believes unauthorised use of the school's computer system may be taking place, or the system may be being used for criminal purposes or storing unauthorised or unlawful text, imagery or sound.

Chapel End Infant School & Early Years Centre School
E-Safety Rules

Parent consent form

All pupils use the computer facilities including Internet access as an essential part of learning, as required by the National Curriculum. Parents/Carers are asked to sign to show that the e-Safety Rules have been understood and agreed.

Parent’s/Carer’s Consent for Web Publication of Work and Photographs

I agree that my son/daughter’s work maybe electronically published. I also agree that appropriate images and video that include my son/daughter may be published subject to the school rule that photographs will not be accompanied by pupil names.

Parent’s/Carer’s Consent for Internet Access

I have read and understood the school e-Safety rules and give permission for my son/daughter to access the Internet. I understand that the school will take all reasonable precautions to ensure that pupils cannot access inappropriate materials but I appreciate that this is a difficult task.

I understand that the school cannot be held responsible for the content of materials accessed through the Internet. I agree that the school is not liable for any damages arising from the use of the Internet facilities.

Signed: Date:

Please print your name:

Name of Child/ren: Class/es:

Please complete, sign and return to the school.

Chapel End Infant School & Early Years Centre School Staff Information Systems Code of Conduct

To ensure that staff are fully aware of their professional responsibilities when using information systems, they are asked to sign this code of conduct. Staff should consult the school's e-safety policy for further information and clarification.

- The information systems are school property and I understand that it is a criminal offence to use a computer for a purpose not permitted by its owner.
- I will ensure that my information systems use will always be compatible with my professional role and in line with guidance within the E-Safety Policy.
- I understand that the school information systems may not be used for private purposes, without specific permission from the head teacher.
- I understand that the school may monitor my information systems and Internet use to ensure policy compliance.
- I will respect system security and will not disclose any password or security information to anyone other than the appropriate system manager.
- I will not install any software or hardware without permission.
- I will ensure that personal data is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely.
- I will respect copyright and intellectual property rights.
- I will report any incidents of concern regarding children's safety to the school e- Safety Coordinator or the Designated Child Protection Officer/Governor.
- I will ensure that any electronic communications with pupils or parents are compatible with my professional role.
- I will promote e-safety with pupils in my care and will help them to develop a responsible attitude to system use and to the content they access or create.

The school may exercise its right to monitor the use of the school's information systems, including Internet access, the interception of email and the deletion of inappropriate materials where it believes unauthorised use of the school's information system maybe taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery and sound.

I have read, understood and agree with the Information Systems Code of Conduct.

Name: Signed:

Date: